Assessing Organizations' Security Journeys:

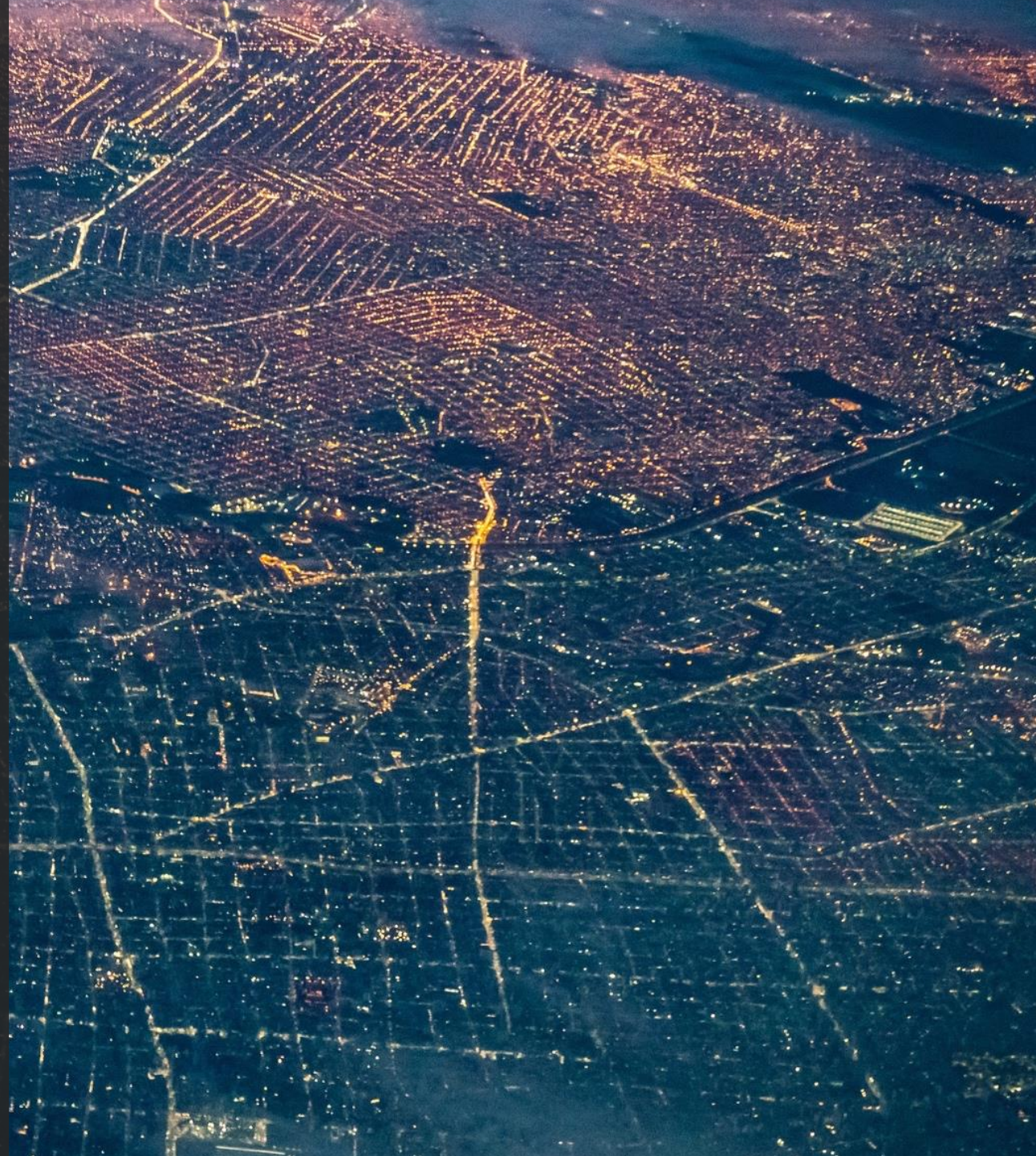
Insights Spanning the Attack Surface, Threat Detection and Response, Attack Recovery, and Zero Trust

Adam DeMattia | Senior Director, Custom Research
Jon Oltsik | Distinguished Analyst & ESG Fellow
Noman Pathan | Market Research Analyst

JANUARY 2024

Table of Contents

Project Overview: Objectives, Methodology, and Next Steps



Enterprise Strategy Group™
by TechTarget

Objectives

- Dell partnered with the Enterprise Strategy Group (ESG) to execute a survey to better understand where organizations are on their security journeys
- The goal of the research to assess where organizations are strongest or weakest across the pillars of attack surface minimization, threat detection and response, and attack recovery
- Additionally, the research seeks to quantify what differentiates organizations having more success in each of these areas from those that are struggling to validate Dell positioning and create opportunities for Dell to make prescriptive recommendations to buyers

Next Steps

- Dell to leverage findings in internal/outbound messaging
- Dell to follow up with ESG with any clarifications or additional asks on the data

Survey Details

QUANTITATIVE WEB-BASED SURVEY

- N=500 qualified completes
- North America (US, Canada, 41%), Western Europe (Germany, UK, 30%), APAC (Australia, New Zealand, Singapore, 29%)
- Field dates: 11/8/2023-11/29/2023

RESPONDENT PROFILE

- Cybersecurity leaders (manager+ titles) knowledgeable about their organization's security posture, processes, and priorities.
- Large midmarket (500 to 999 employees, 30%) and enterprise (1,000+ employees, 70%) organizations
- Multiple industry verticals including manufacturing, financial, retail/wholesale, and healthcare, among others
- Complete demographics included at end of presentation

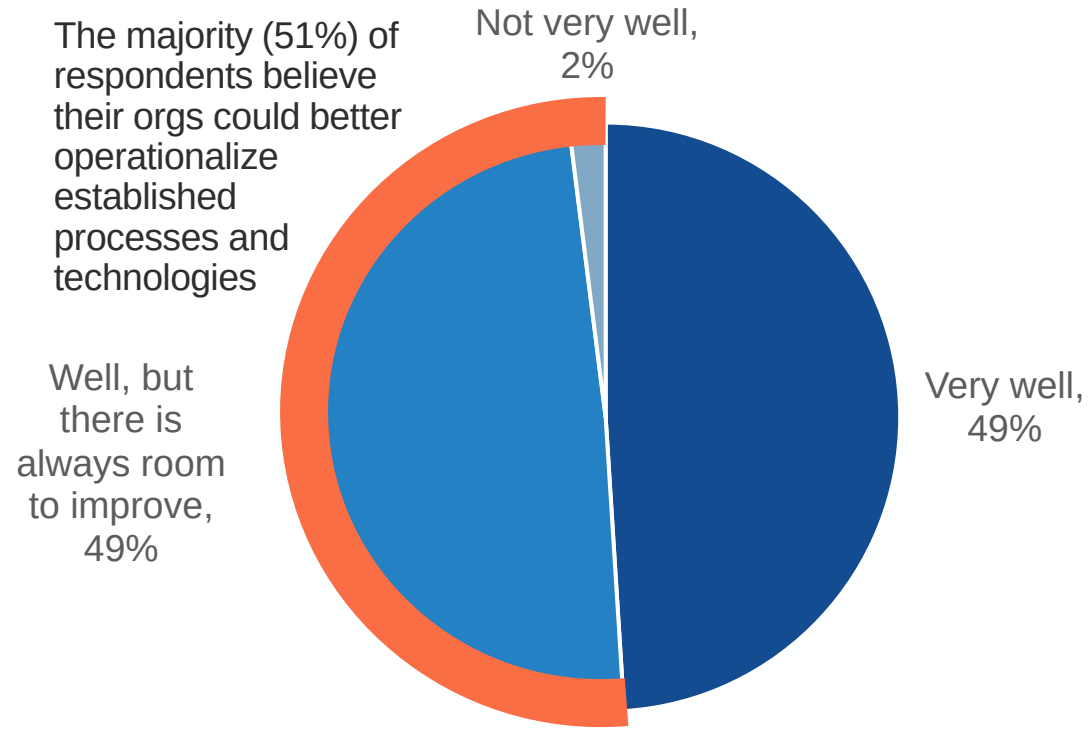
The Aggregate View of the Cybersecurity Program

Enterprise Strategy Group™
by TechTarget

Cybersecurity Program Maturity Is a Work in Progress for Most

Only 29% of organizations represented have both the right policies and technologies in place *AND* can operationalize them very well.

Question text: How would you characterize the maturity level of your organization's cybersecurity program? (Percent of respondents, N=500)

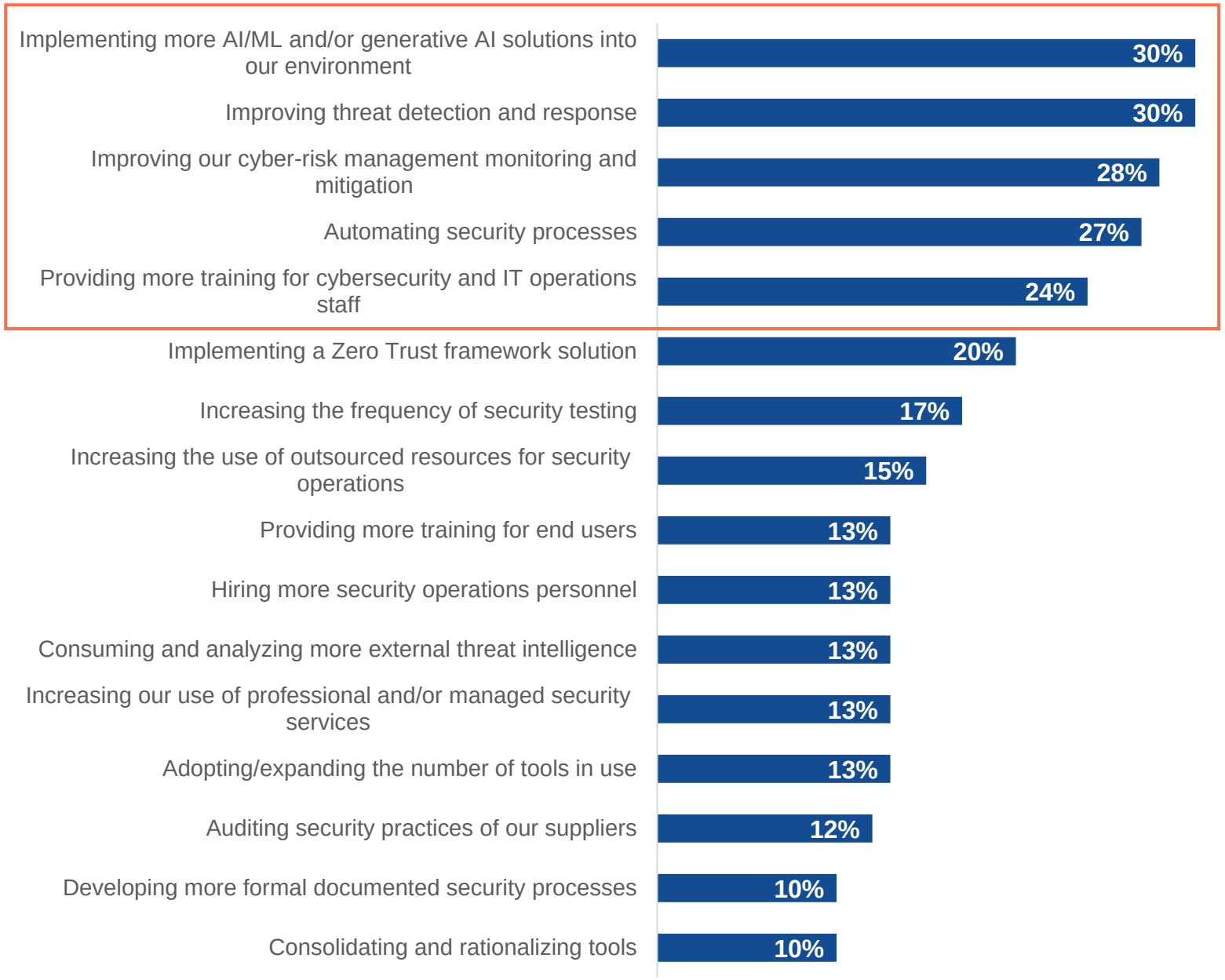


Question text: How well does your organization operationalize its security policies, processes, and technologies? (Percent of respondents, N=475)

What Organizations Are Prioritizing Looking Ahead to 2024

Implementing more AI, improving TDR, getting a stronger handle on cyber risk, automation, and technical team training are in the top tier of organizational priorities.

C-level respondents were much more likely to prioritize AI/ML implementation than less senior managers (41% vs. 27% of management).



Question text: As part of its overarching cybersecurity strategy, which of the following actions will your organization most prioritize over the next year? (Percent of respondents, N=500, three responses accepted)

Challenges Organizations Are Most Often Grappling With

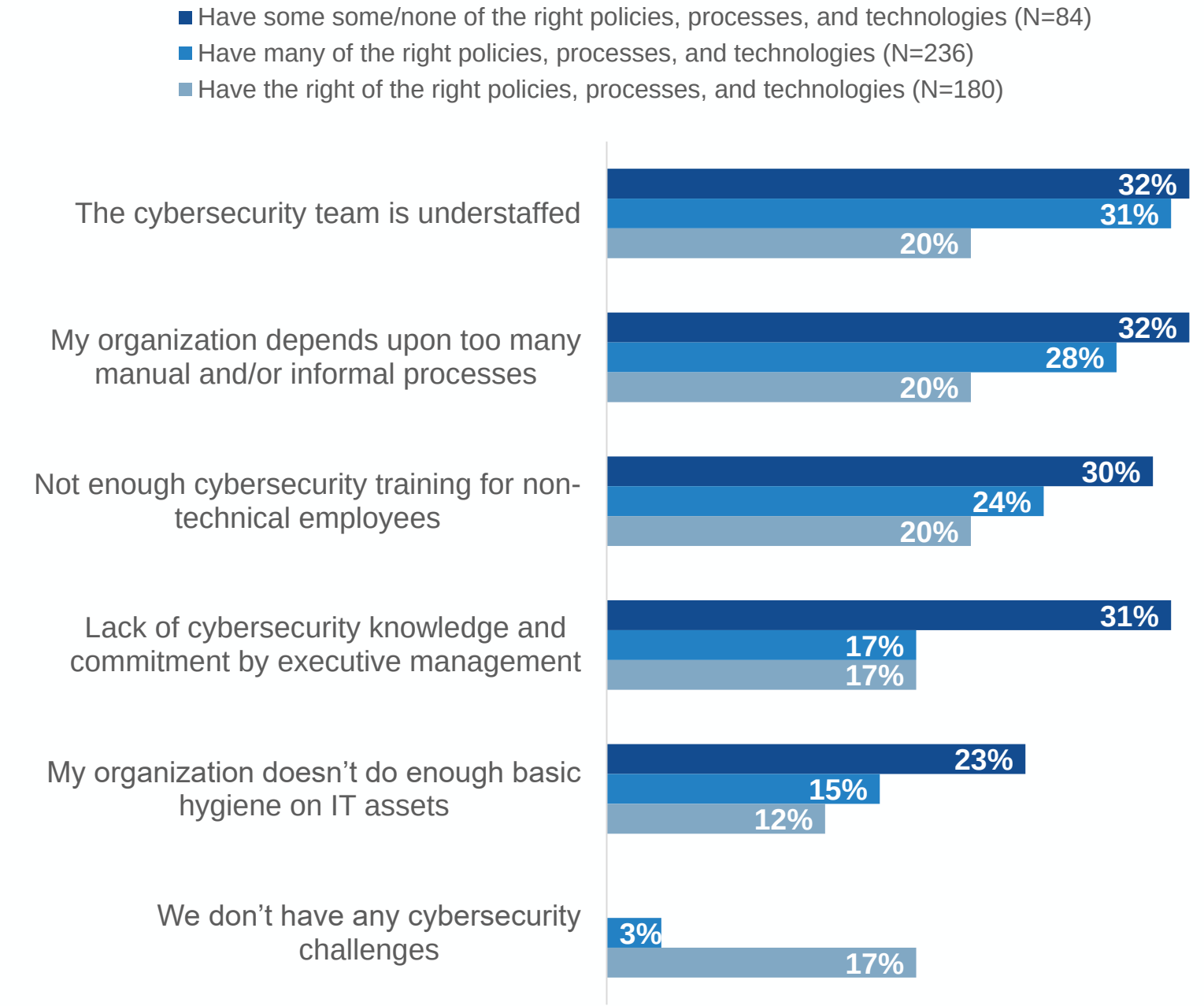
Challenges most often top-of-mind include alert volumes, tool complexity, staffing issues (both scale and expertise), and too many manual processes.

The cumulative impact of these interrelated challenges puts organizations in a tough position.

Question text: Which of the following would you say are the biggest cybersecurity challenges at your organization? (Percent of respondents, N=500, three responses accepted)

Cybersecurity Challenges Cut, by Program Maturity

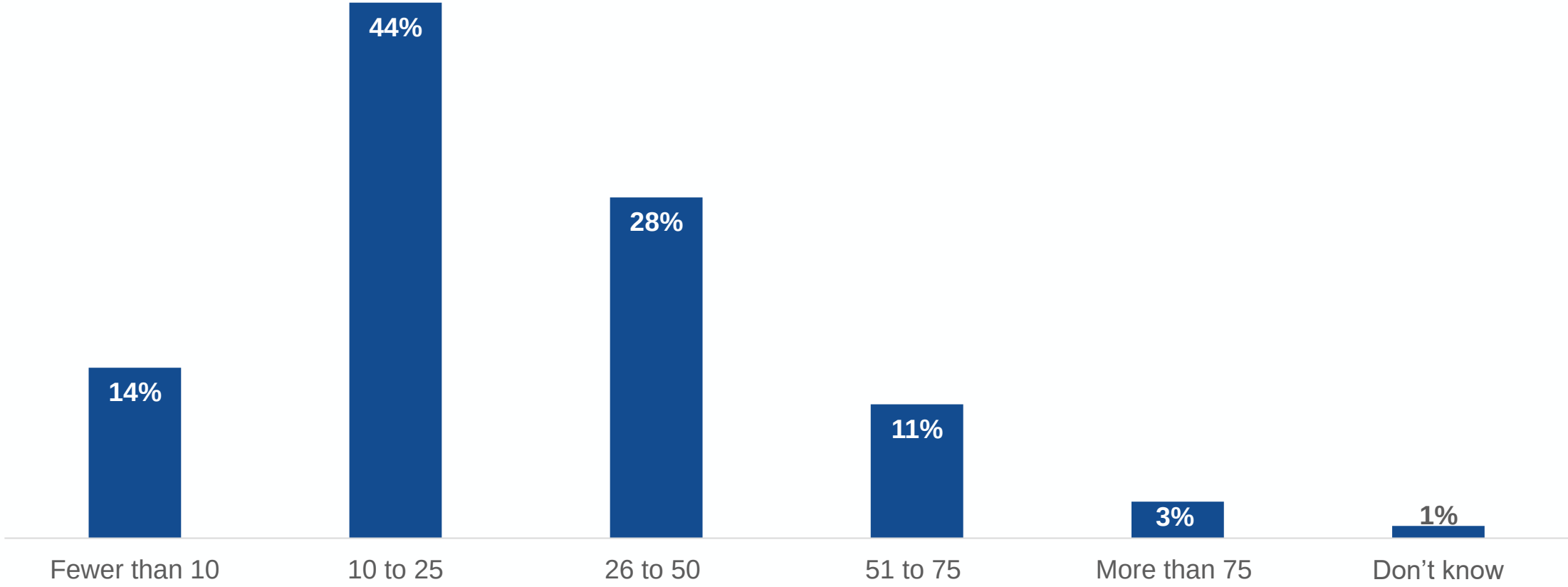
As organizations mature their cybersecurity programs, the tend to solve many key issues.



Question text: Which of the following would you say are the biggest cybersecurity challenges at your organization?(Percent of respondents, up to three responses accepted)

How Complex Are Organizations' Security Tool Ecosystems?

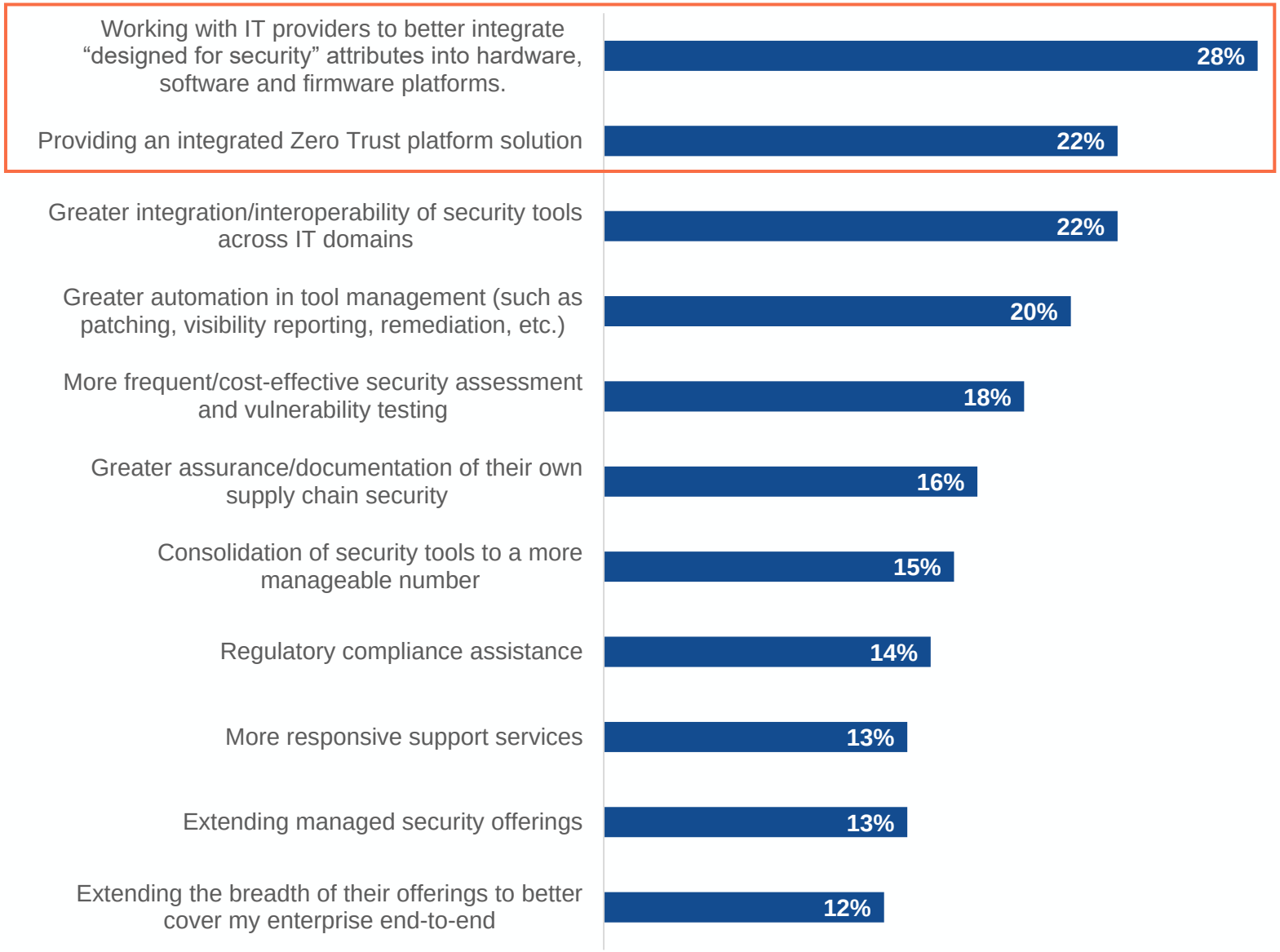
On average, respondents report their organization has ~29 different security tools in use; cyber program maturity is correlated to more tools being in use: organizations with the right policies, processes, and technologies in place have ~15% more tools deployed (30.5 vs. 26.5). Enterprises (1,000+ employees) similarly have more solutions deployed vs. their large midmarket counterparts (i.e., 500-999 employees; estimated means of 32 vs. 22.5)



Question text: Approximately how many different security tools and technologies (i.e., commercial, homegrown, open source, etc.) are used at your organization? (Percent of respondents, N=500)

What Respondents Want Most from Vendors

Dell is well positioned to help customers in ways they want to be helped.

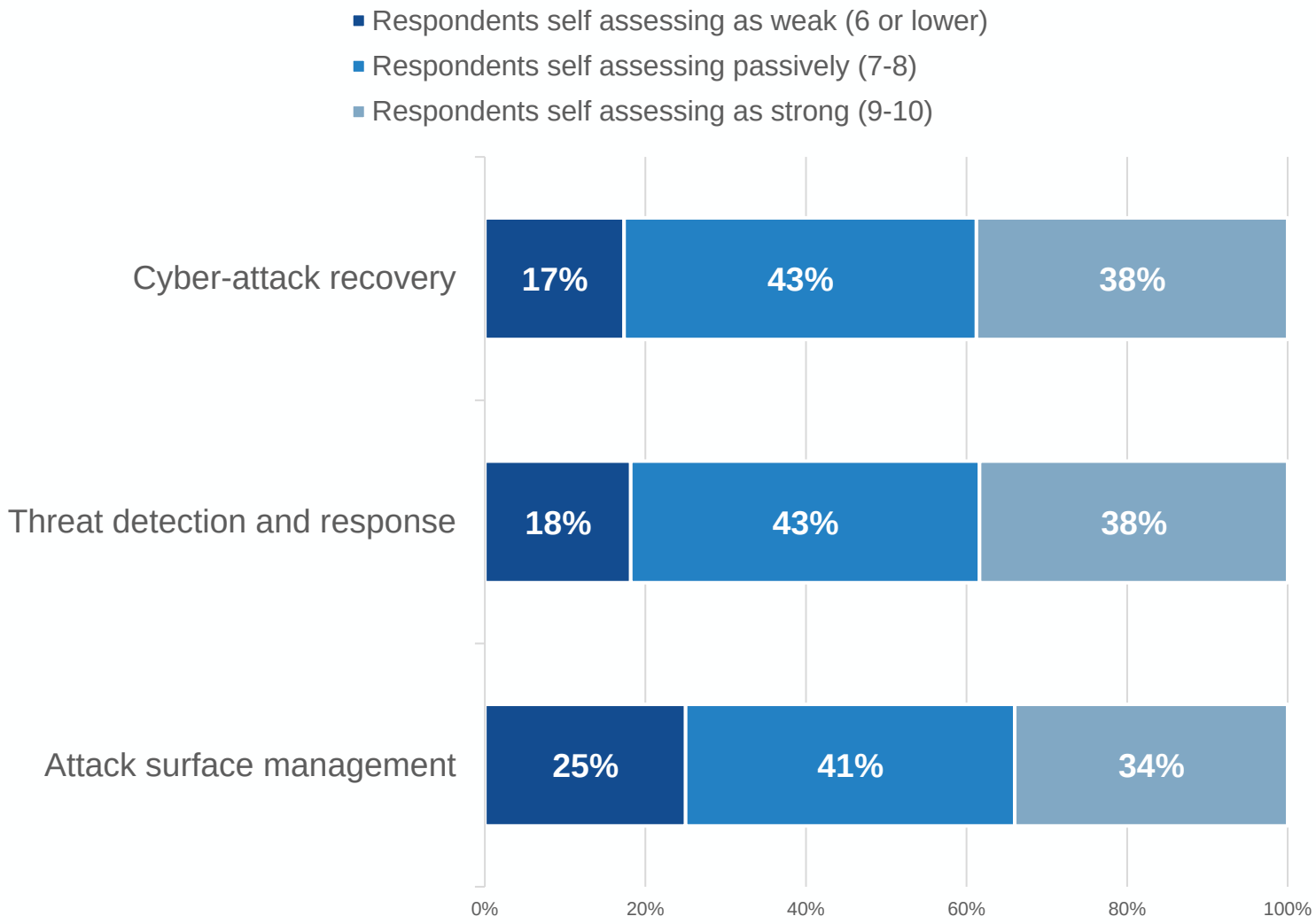


Question text: What improvements could third-party security providers make that would be most useful to your organization’s security initiatives? (Percent of respondents, N=401, two responses accepted)

Respondents' Assessment of Cybersecurity Program Pillar Strength

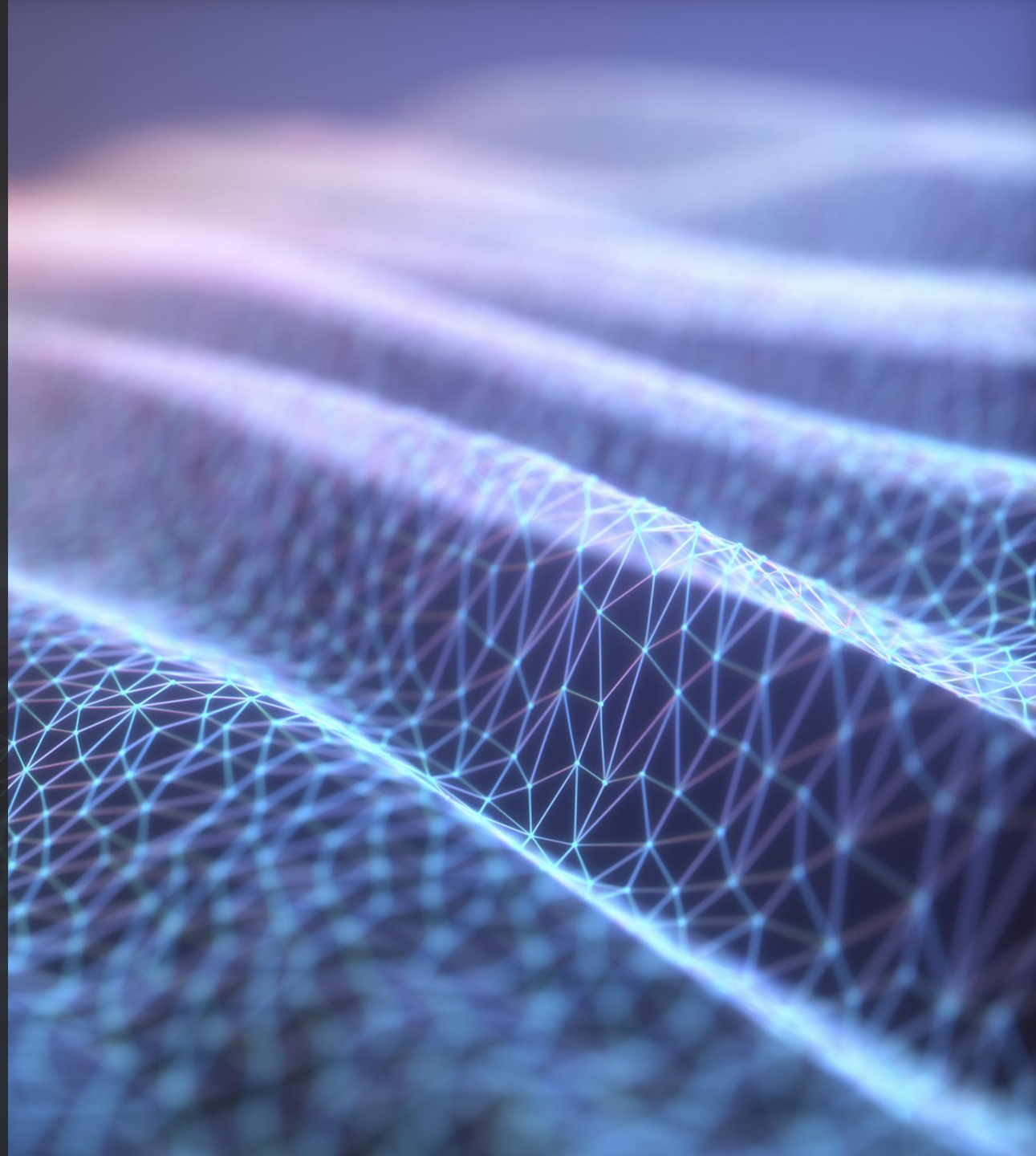
While the difference isn't stark, respondents most often report weakness in the area of attack surface management.

This categorization is inspired by NPS advocacy benchmarking approaches and is used to uncover differences in organizations' approaches that help explain ***why*** some organizations have more success and to create opportunities for "Learn form the leaders" messaging, better account segmentation.



Question text: In your opinion, how would you describe your organization's approach to attack surface management, threat detection and response, and cyber-attack recoveries? (Percent of respondents, N=500)

Attack Surface Deep Dive



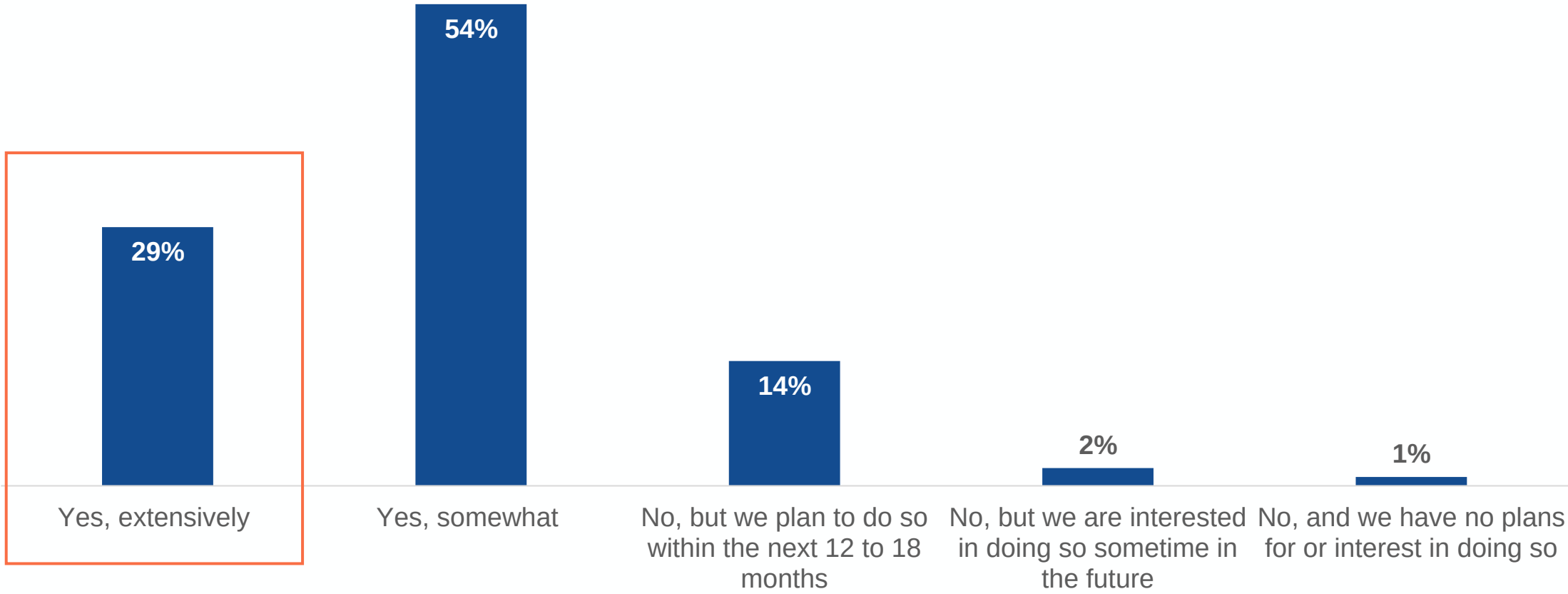
Enterprise Strategy Group™
by TechTarget

Highlighted Findings: Attack Surface Deep Dive

- **There is a correlation between automation and attack surface management strength:** Orgs with the best attack surface management capabilities are 3x more likely than those that are weak to have extensively automated operations (49% vs. 16%).
- **Similarly, the (perceived) adoption of AI and GenAI is also correlated to attack surface management strength.**
- **91% of organizations agree that reducing the attack surface requires a cross-functional focus, 88% agree that automating attack surface reduction tasks is critical, 89% of organizations are applying new technologies to the problem, and 87% are partnering with service providers to help.**
- While attack surface management challenges are varied, the fact that **securing the IT hardware supply chain took the top spot** shows a key Dell value prop is well aligned to a challenge many organizations grapple with.
- Validating Dell's PoV, **the majority of respondents say** endpoint security features that **protect end user credentials from malware, automate BIOS IoCs, and validate configurations from the factory** are each **critically important.**
- **Leaders on ASM more often** report an intention to **partner with testing service providers** and to **increase their testing budget**.

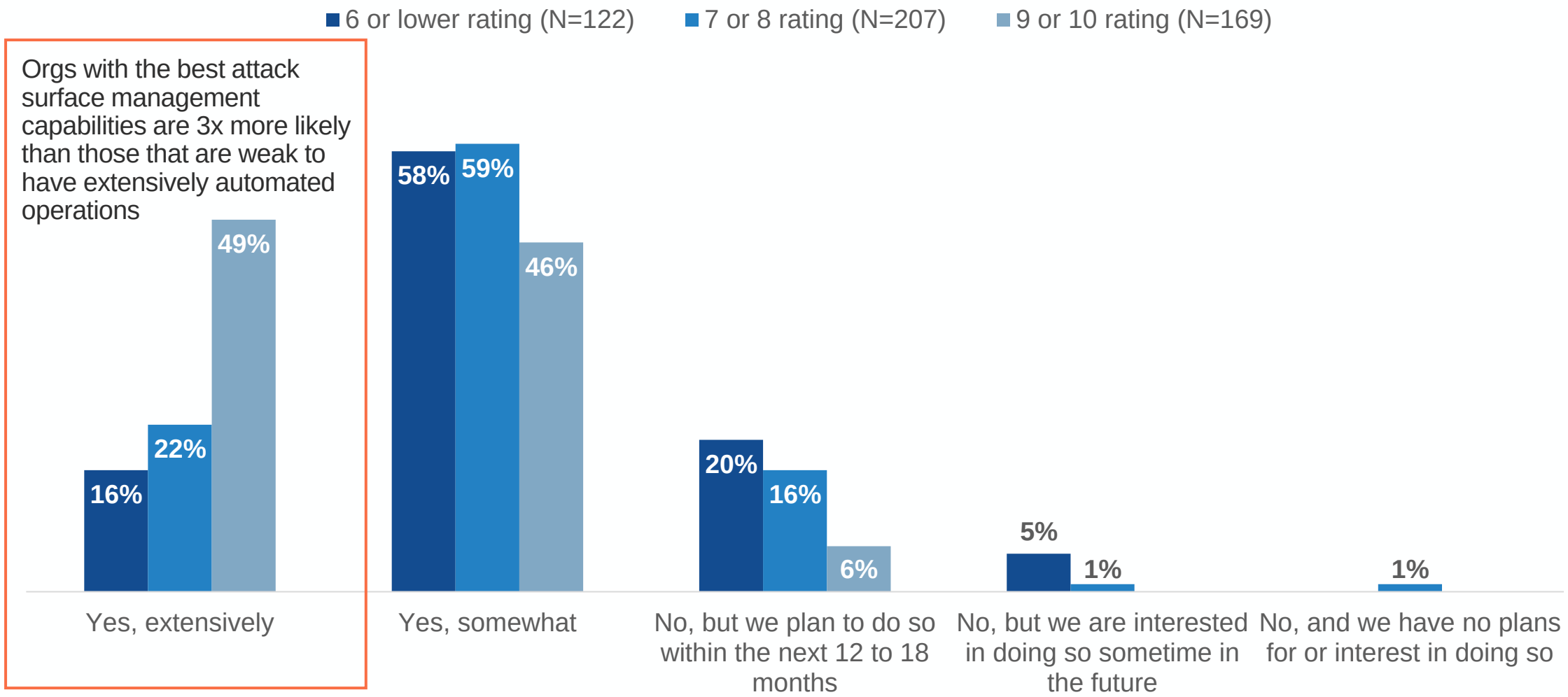
Automating attack surface reduction activities is an on-going process for most organizations

Only 29% of organizations have “extensively” automated attack surface reduction activities, but the majority (54%) report some progress.



Question text: Has your organization automated attack surface reduction activities? (Percent of respondents, N=500)

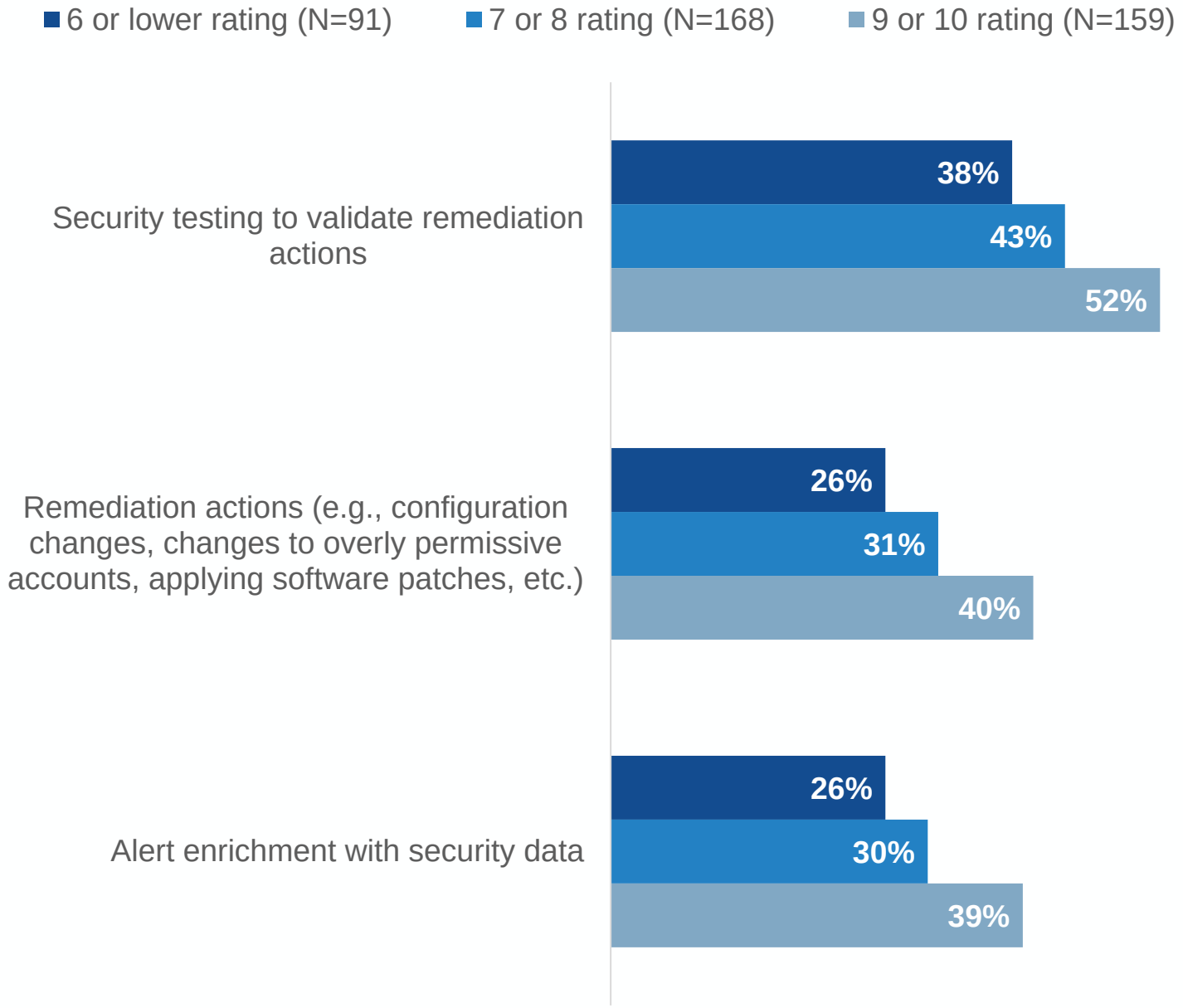
Strength in Reducing the Attack Surface Is Strongly Correlated with Attack Surface Management Automation



Question text: Has your organization automated attack surface reduction activities? (Percent of respondents)

Select Differences in the Propensity to Have Successfully Automated Attack Surface Management Tasks, by Attack Surface Management Capabilities

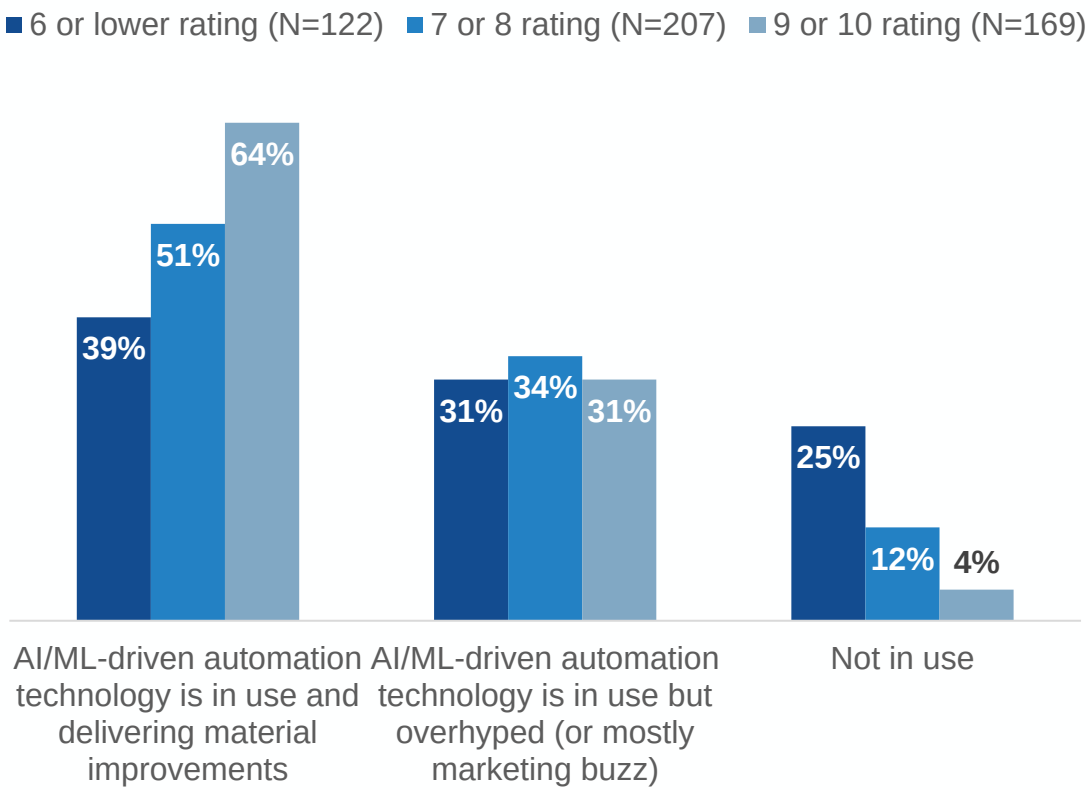
Leaders in attack surface management were much more apt to report successfully automating three key attack surface management tasks.



Question text: Which of the following attack surface reduction activities has your organization automated successfully (e.g., human effort has been materially reduced but effectiveness has been increased)? (Percent of respondents, multiple responses accepted)

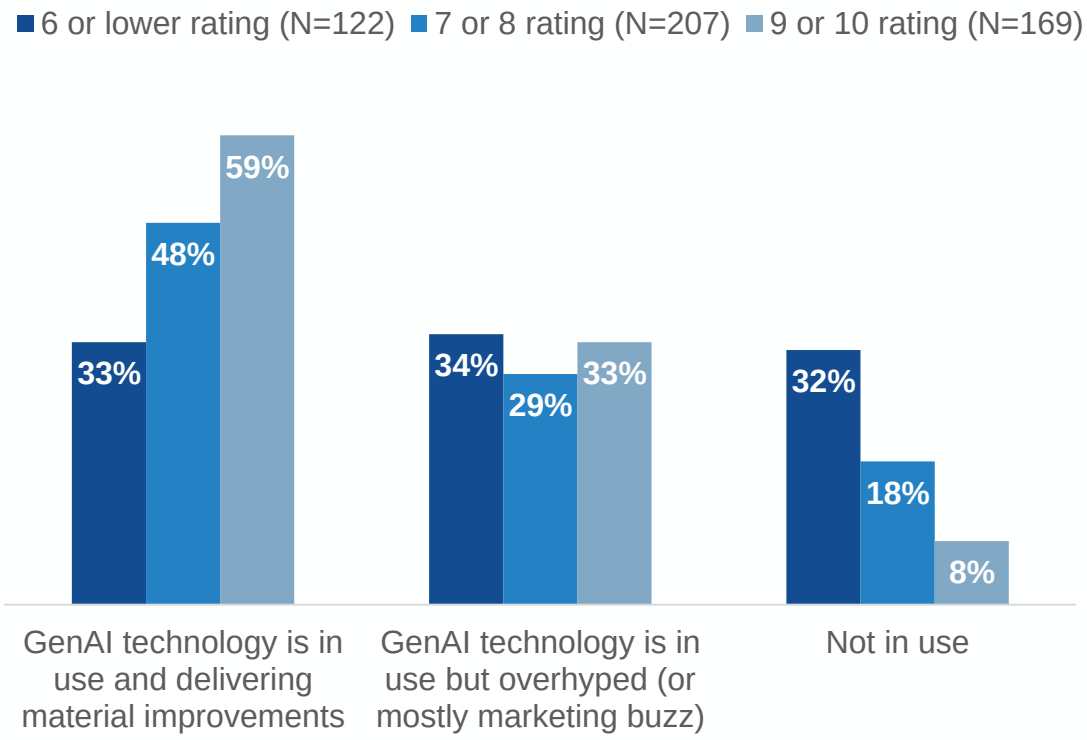
Organizations' Application of AI Technologies to Manage/Minimize the Attack Surface

Use of AI/ML-driven automation technologies



Question text: What best describes the use of artificial intelligence/machine learning-driven automation technology for attack surface management at your organization? (Percent of respondents)

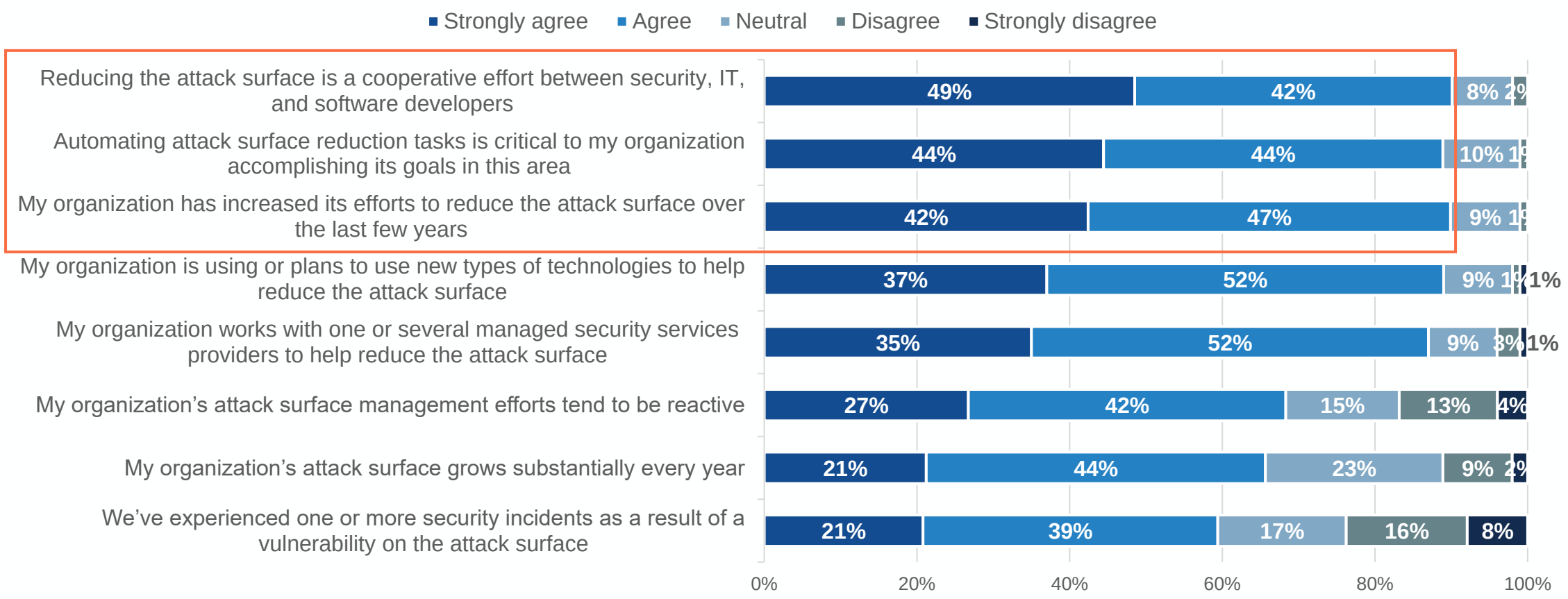
Use of GenAI technologies



Question text: What best describes the use of GenAI technology for attack surface management at your organization? (Percent of respondents)

Agreement with a Multitude of Statements Related to the Attack Surface Run High

91% of organizations agree that reducing the attack surface requires a cross-functional focus, 88% agree that automating attack surface reduction tasks is critical, and 89% of organizations are leaning in to reducing the attack surface

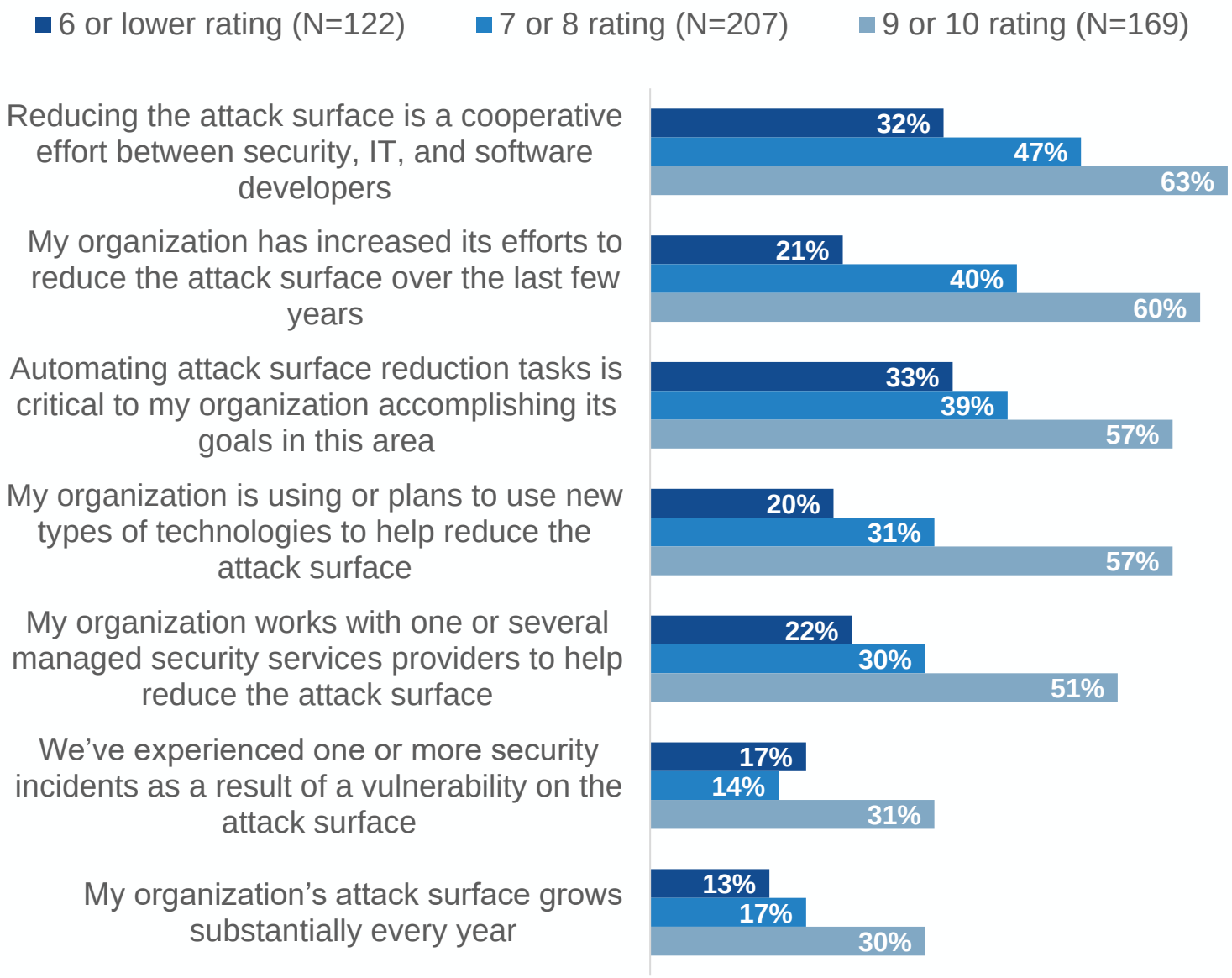


Question text: Please rate your level of agreement with each of the following statements. (Percent of respondents, N=500)

An Organization's Attack Surface Management Effectiveness Is Closely Correlated to Several Perceptions and Actions

Organization's most effective at managing the attack surface are:

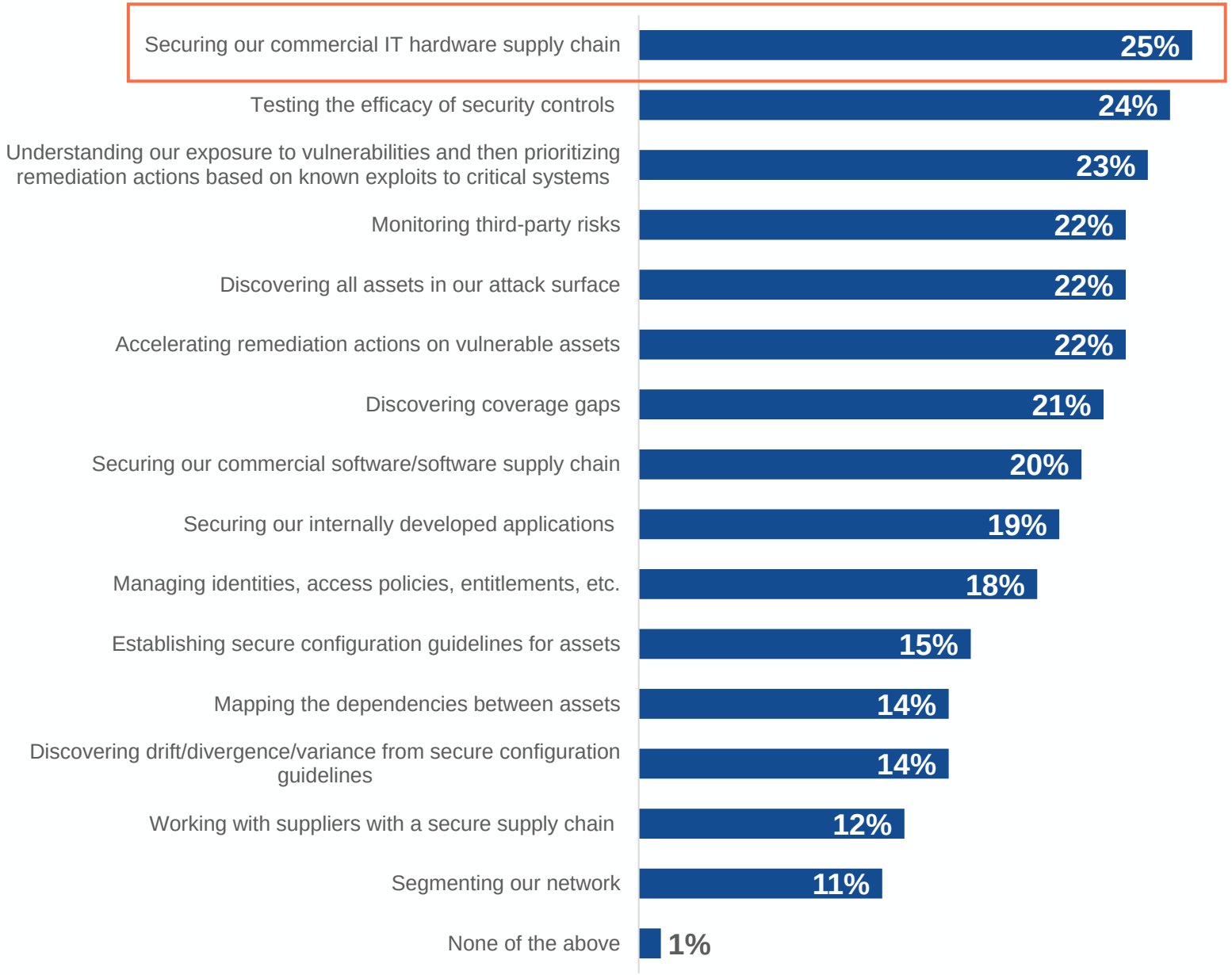
- 2.9x as likely to have increased their efforts in this area over the past few years
- 2.9x as likely to be investing in new/innovative technologies to help
- 2.3x as likely to be partnering with service providers to help with attack surface reduction
- And more



Question text: Please rate your level of agreement with each of the following statements.: (Percent of respondents, "Strongly agree" respondents)

Challenges with reducing attack surface

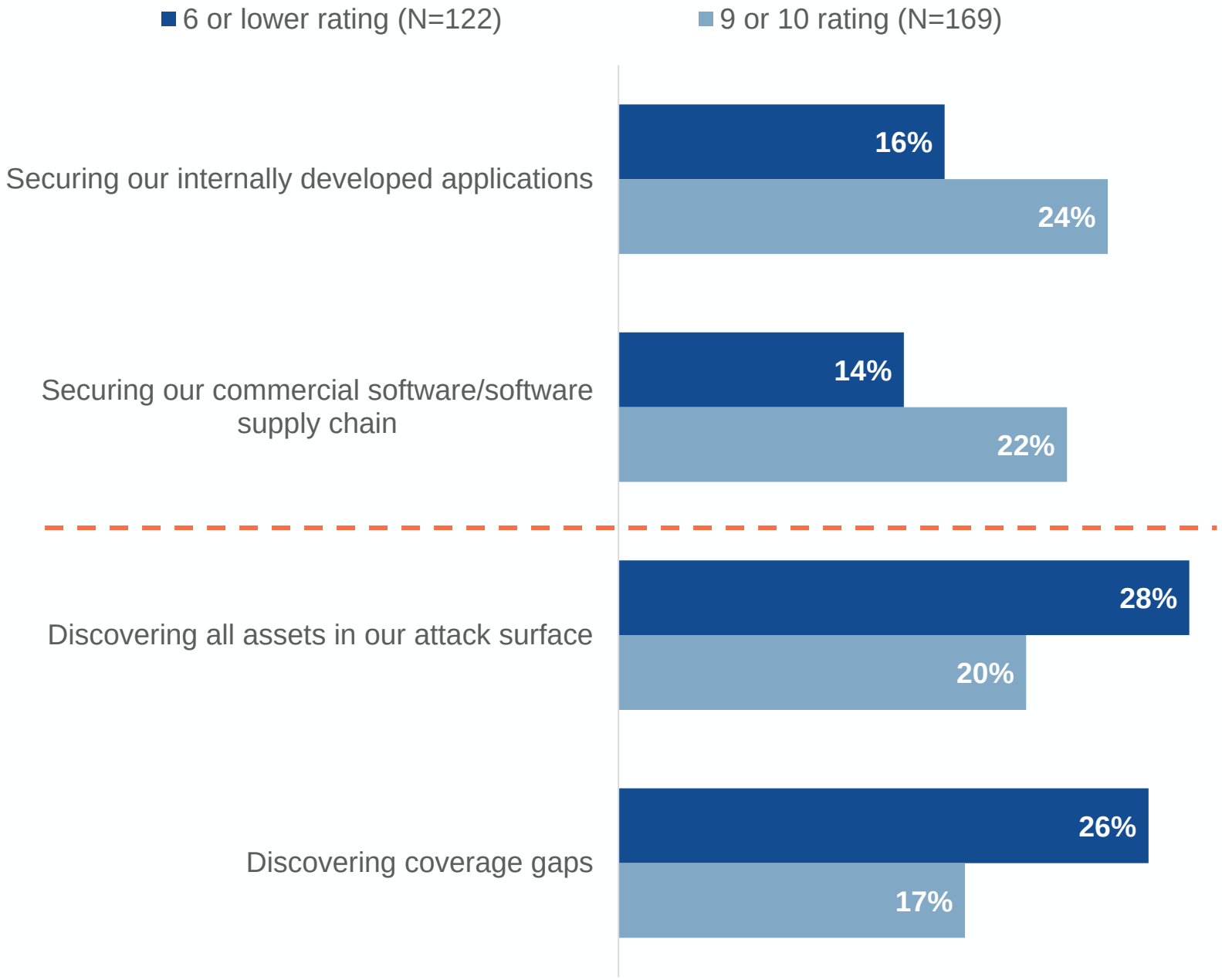
While the attack surface management challenges are varied, the fact that securing the IT hardware supply chain took the top spot shows a key Dell value prop is well aligned to a challenge many organizations grapple with.



Question text: Which of the following activities related to reducing the attack surface are most challenging for your organization? (Percent of respondents, N=500, three responses accepted)

Select Differences in Challenges, by Attack Surface Management Capabilities

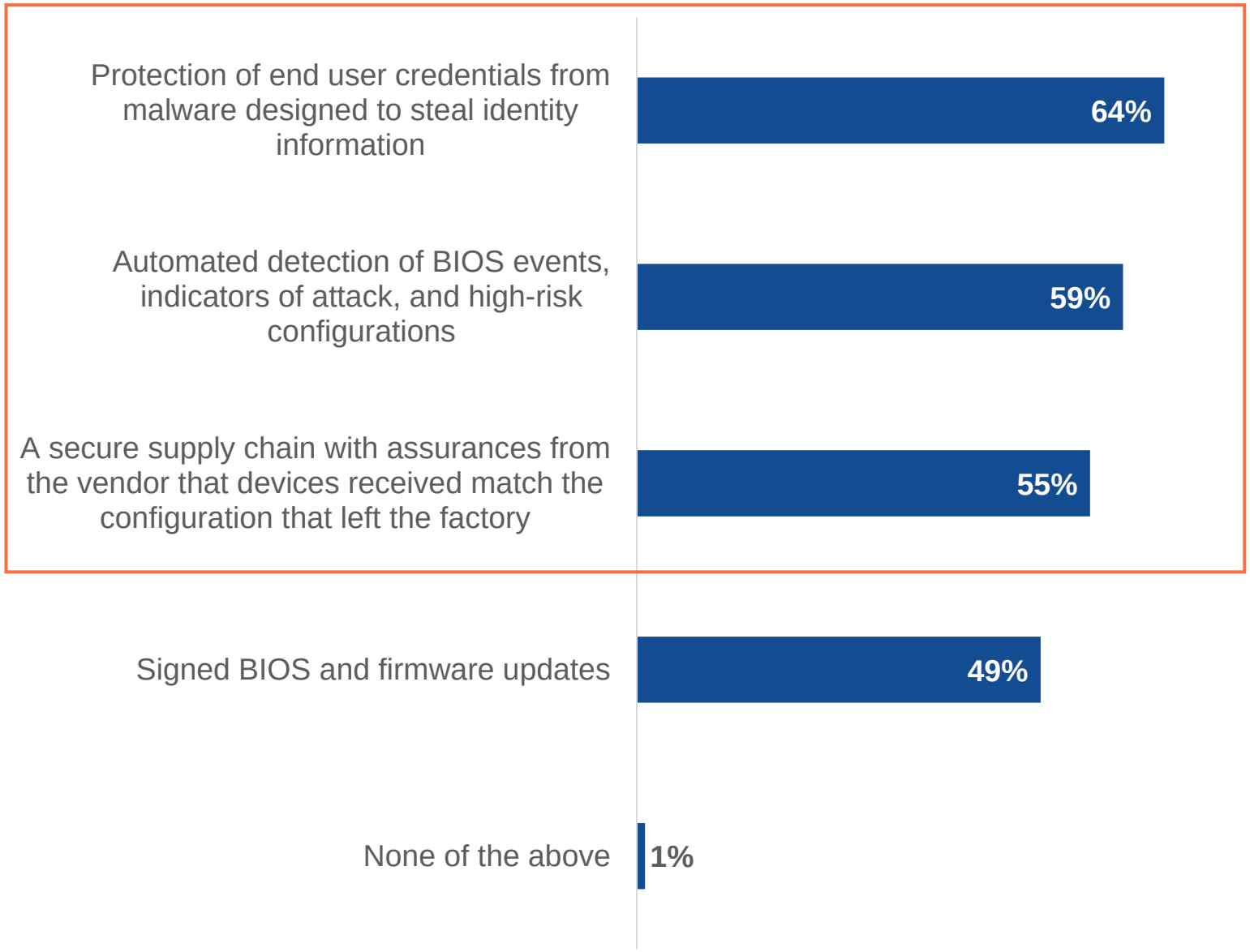
Organizations strong on attack surface management more often struggle with securing the software supply chain; Organizations weak on attack surface management more often struggle with imperfect visibility.



Question text: Which of the following activities related to reducing the attack surface are most challenging for your organization? (Percent of respondents, up to three responses accepted)

Evaluation Criteria in New Endpoint Technologies

Validating Dell's PoV, the majority of respondents say endpoint security features that protect end user credentials from malware, automate BIOS IoCs, and validate configurations from the factory are each critically important.

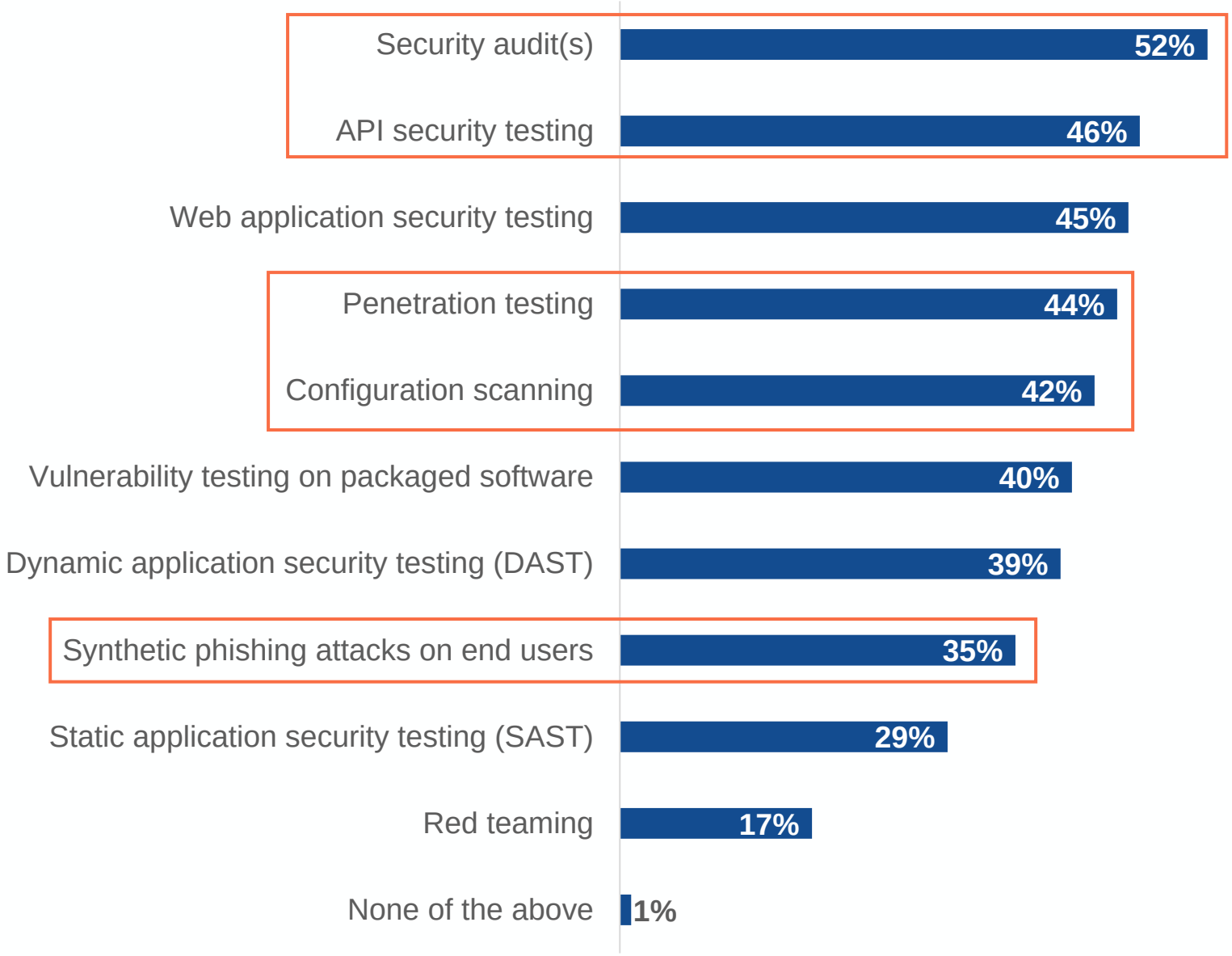


Question text: When your organization is evaluating investments in new endpoint technologies (e.g., client devices, server, etc.), which of the following security features are considered critically important? (Percent of respondents, N=500, multiple responses accepted)

Methods of Security Testing Employed on a Regular Cadence

The number of security tests performed vary by organizations' size as enterprises are significantly more likely to conduct:

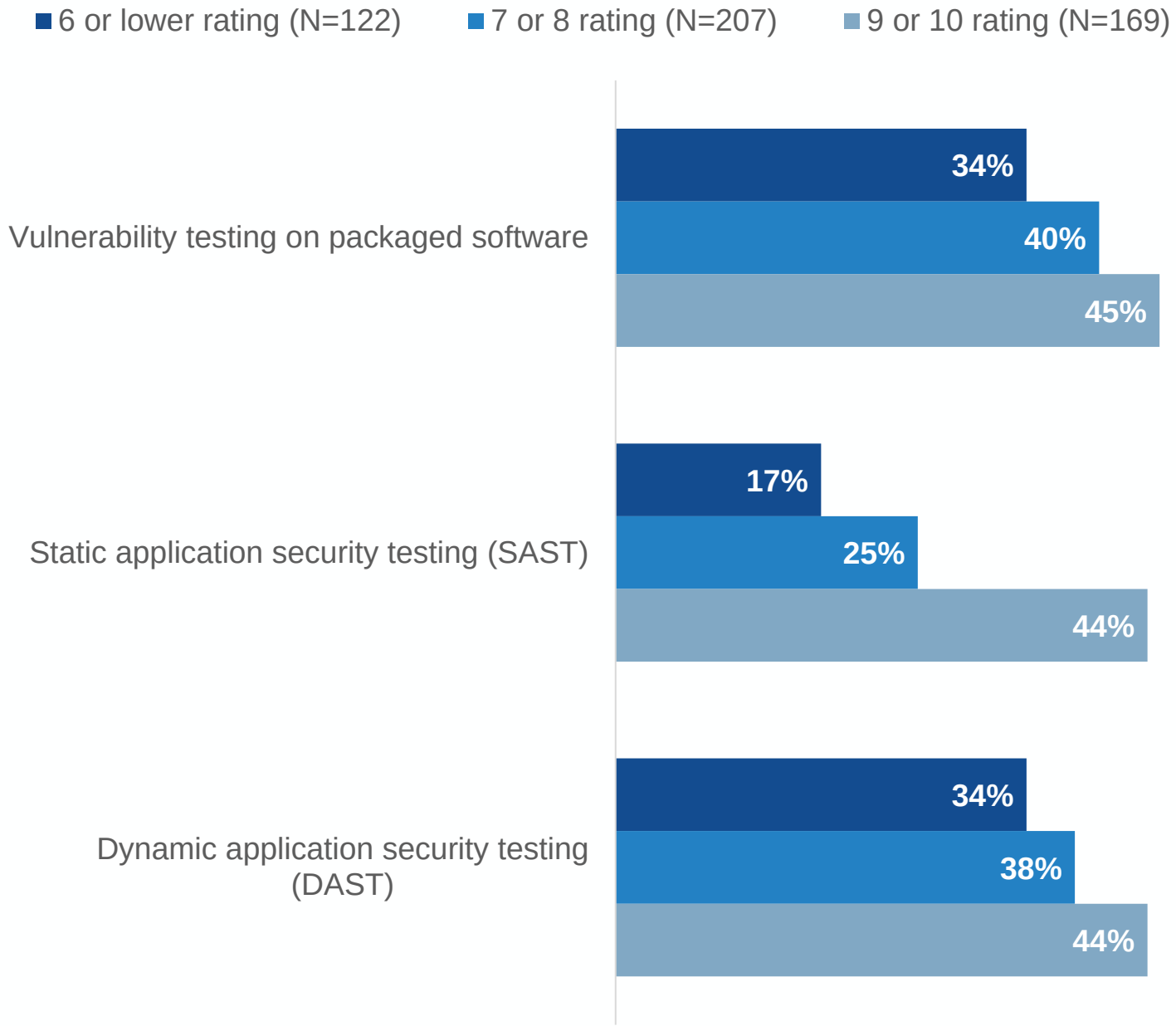
- Synthetic phishing attacks on end users (37% vs. 28% of SMBs).
- Penetration testing (46% vs. 37% of SMBs).
- API security testing (50% vs. 36% of SMBs).
- Configuration scanning (45% vs. 34% of SMBs).
- Security audits (55% vs. 45% of SMBs).



Question text: Which of the following best reflects the security testing your organization currently performs on a regular cadence? (Percent of respondents, N=500, multiple responses accepted)

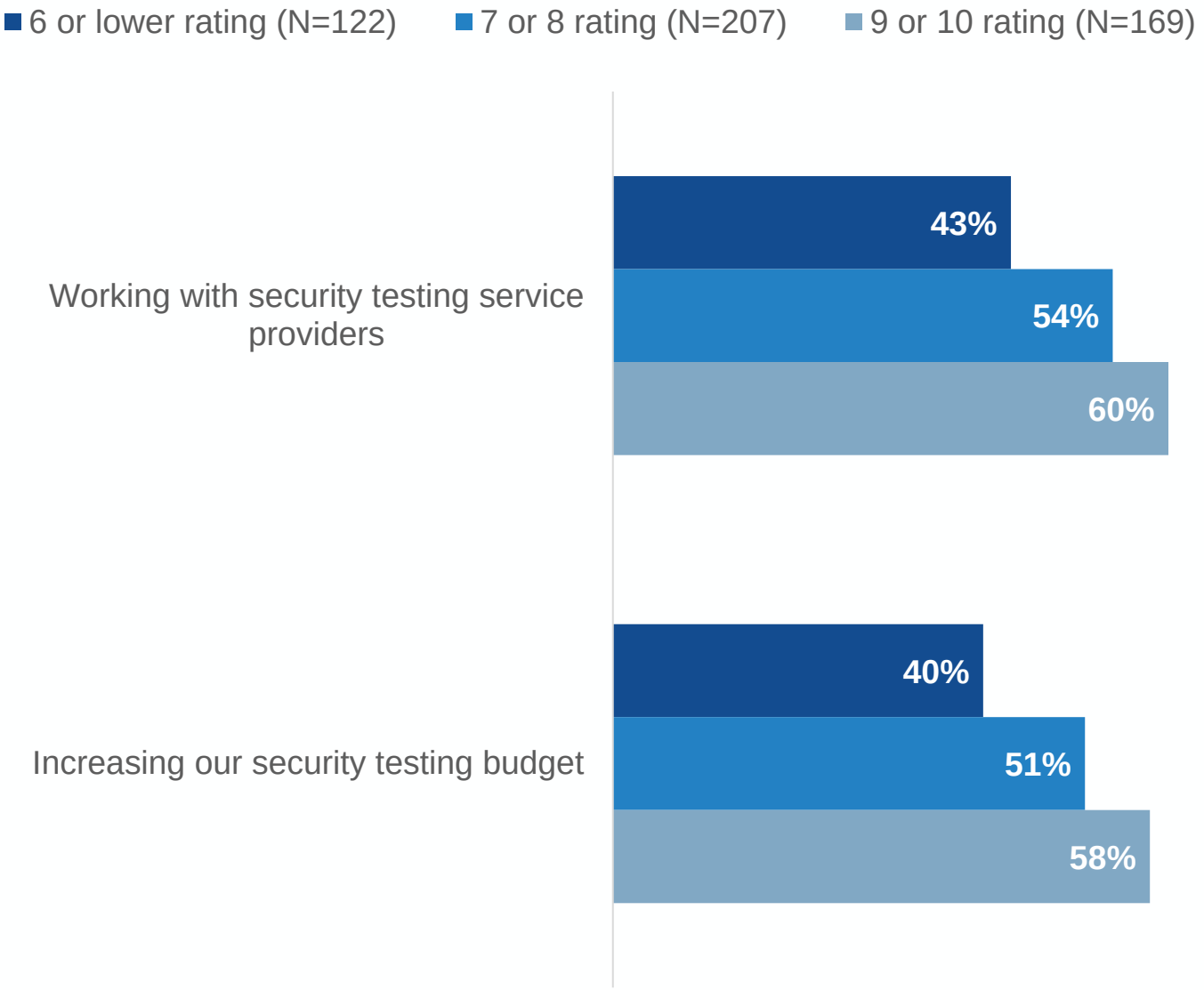
Three Testing Methodologies Leaders More Frequently Employ

Organizations that are strong on attack surface management are 32% more likely to regularly test packaged software for vulnerabilities, 29% more likely to leverage DAST, and 2.6x as likely to employ SAST.



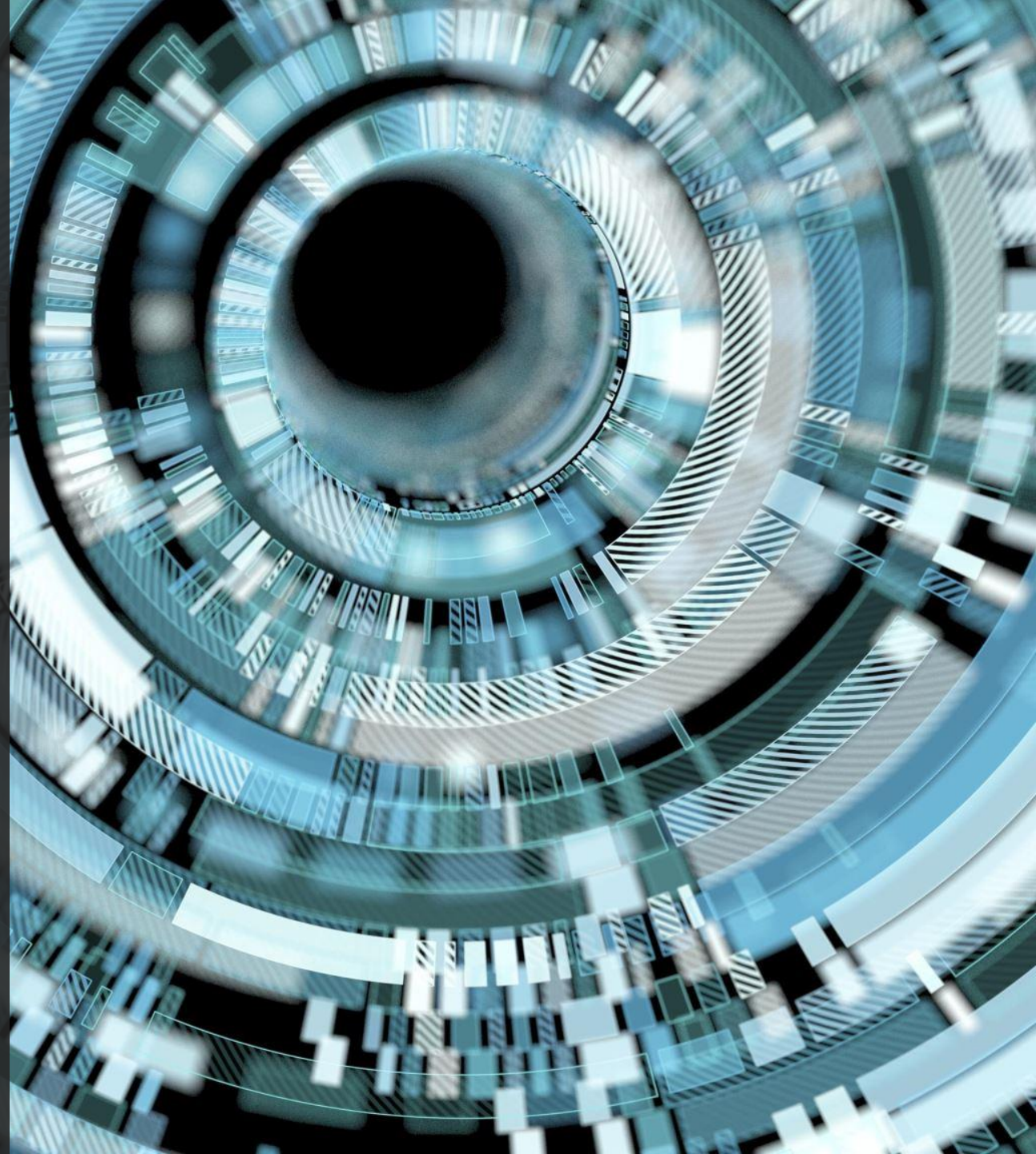
Question text: Which of the following best reflects the security testing your organization currently performs on a regular cadence? (Percent of respondents, multiple responses accepted)

Leaders More Often Report an Intention to Partner with Testing Service Providers and Increasing their Testing Budget



Question text: What is your organization doing over the next 12 months to improve security testing? (Percent of respondents, multiple responses accepted)

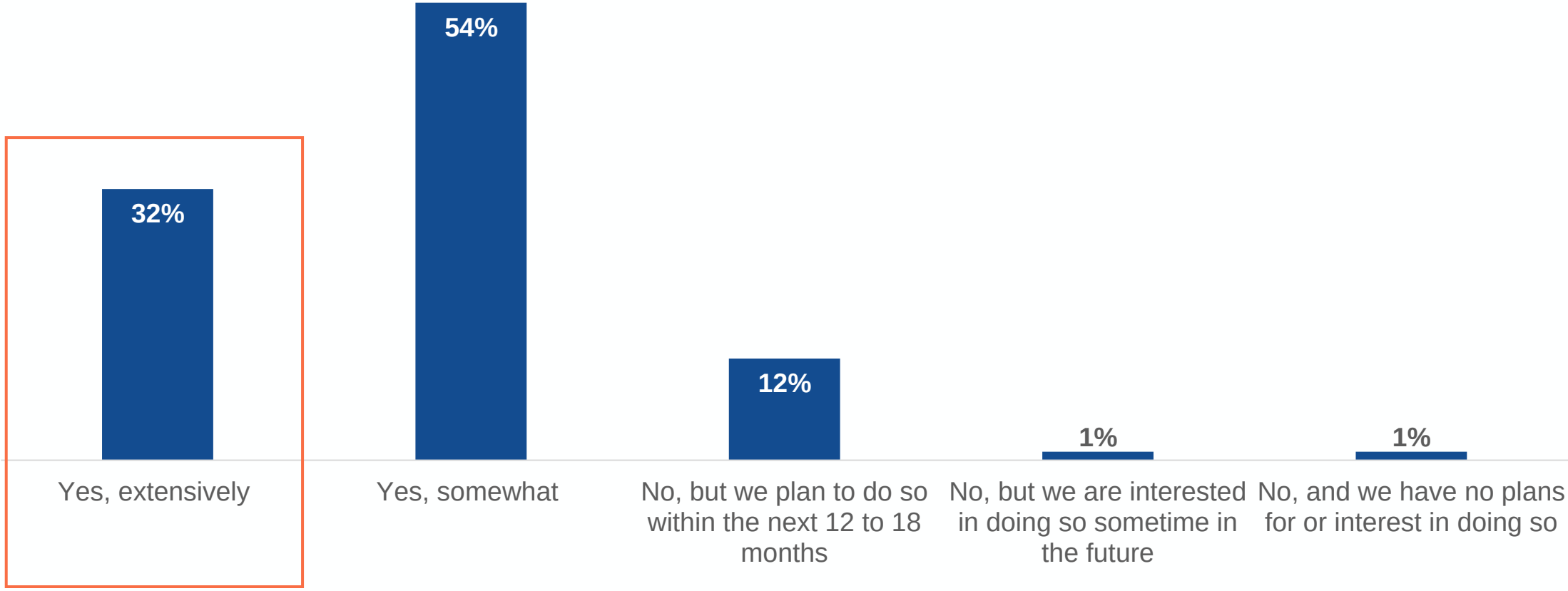
Threat Detection and Response Details



Enterprise Strategy Group™
by TechTarget

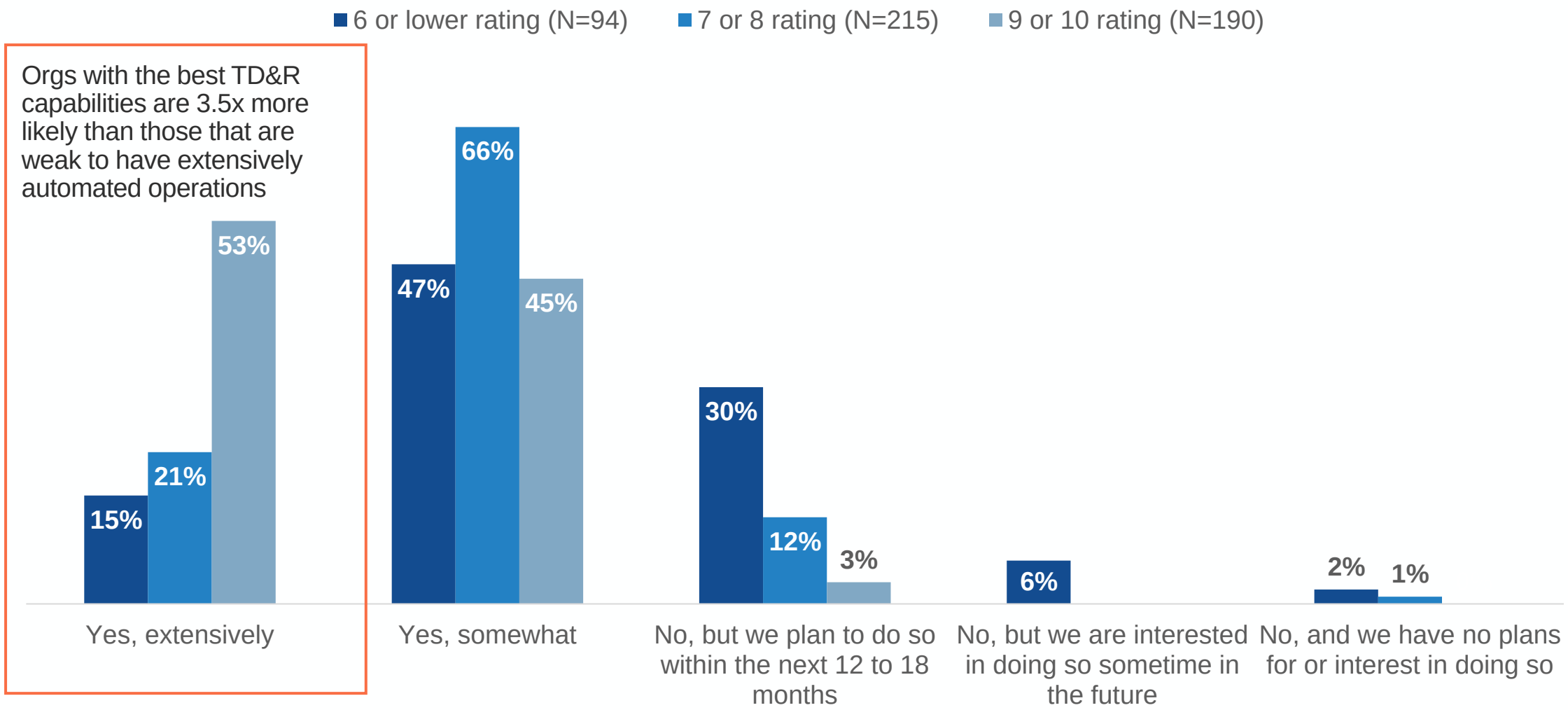
TD&R Automation Is in a Similar State to Attack Surface Management Automation

Less than a third (32%) of organizations have indicated they have extensively automated TDR activities.



Question text: Has your organization automated threat detection and response activities? (Percent of respondents, N=500)

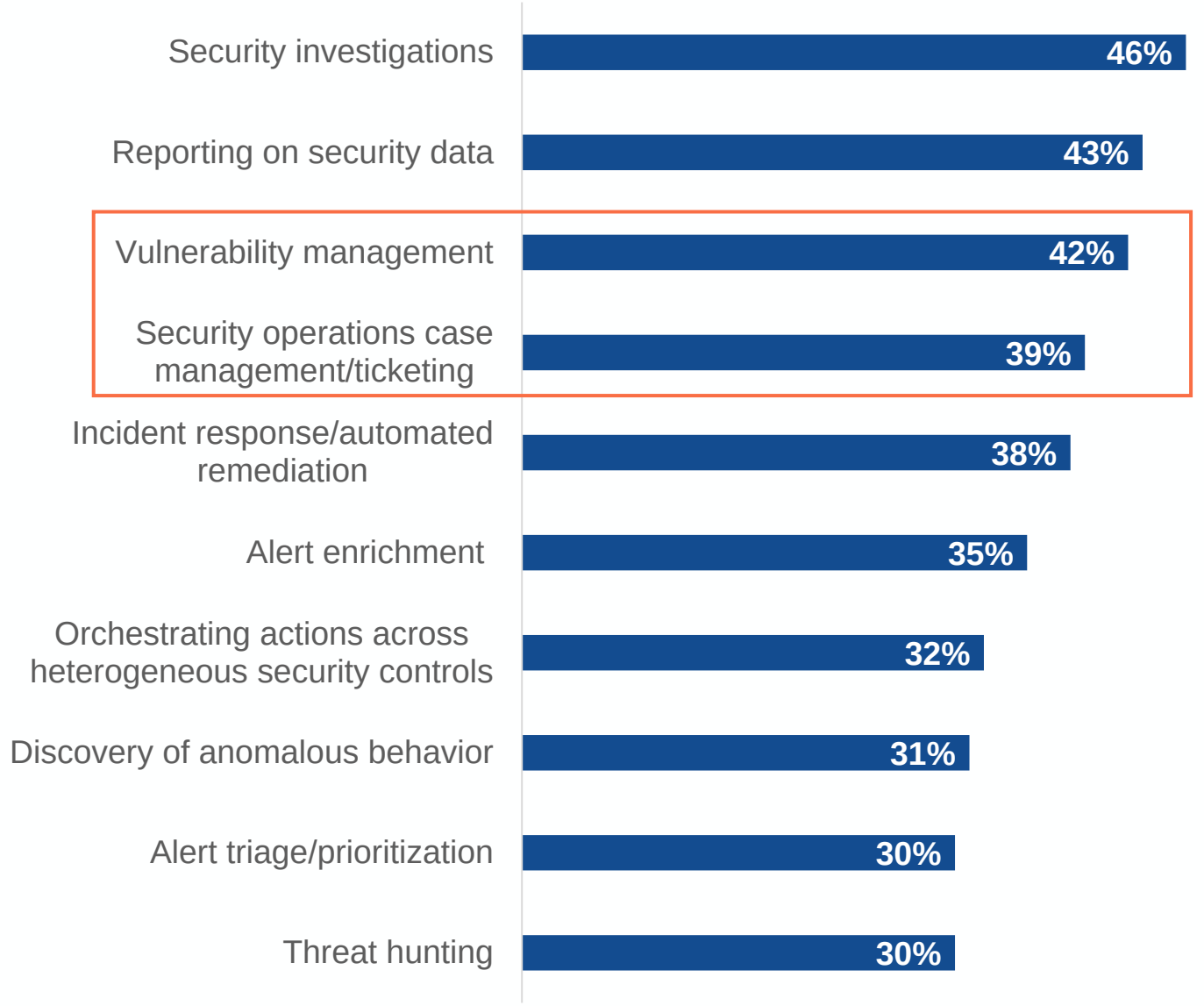
Strength in TDR Is Strongly Correlated with TD&R Automation



Question text: Has your organization automated threat detection and response activities? (Percent of respondents)

TD&R Activities Organizations Have Successfully Automated

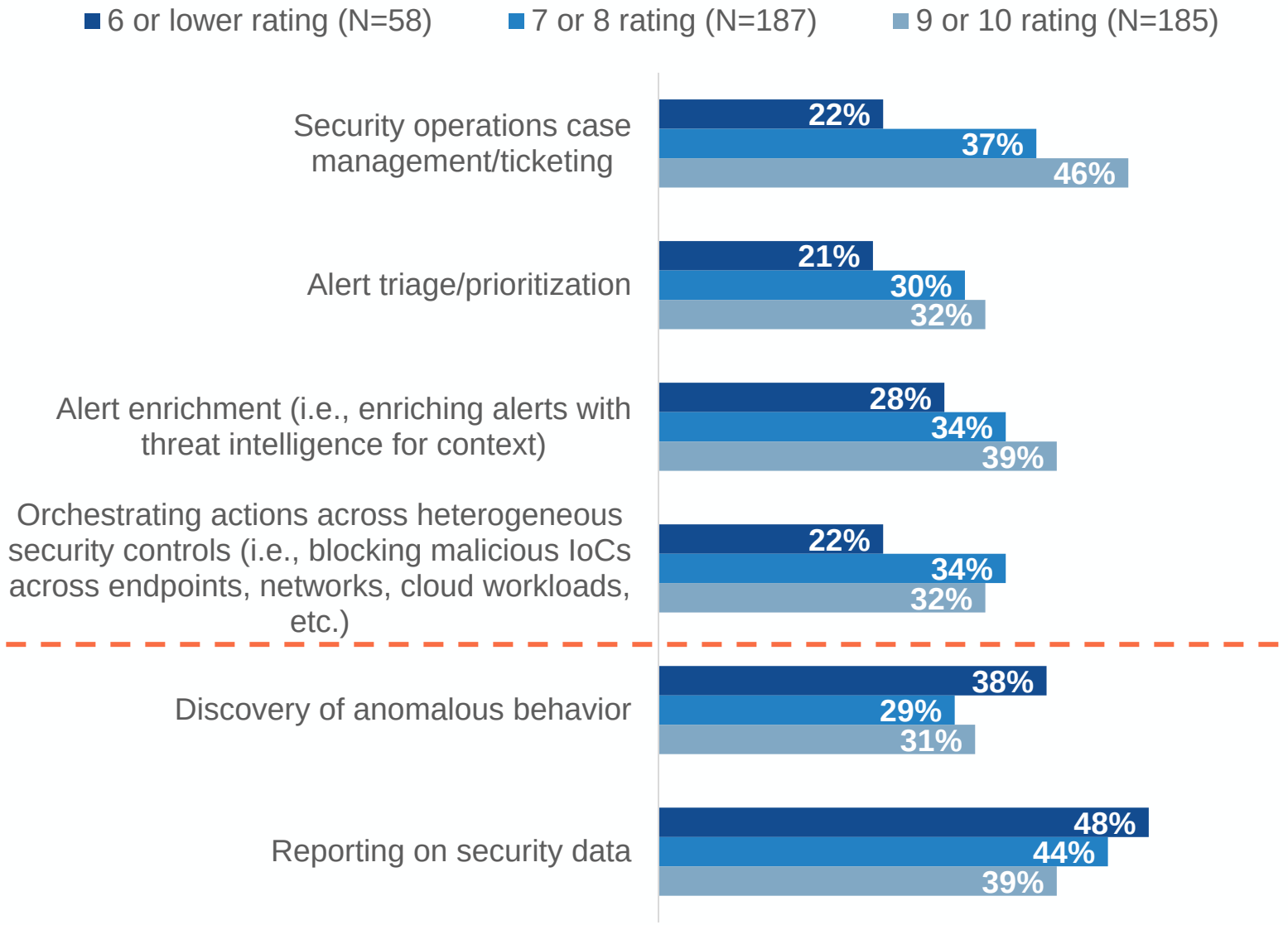
TD&R automation activities vary by organization size as enterprise are more likely to have automated vulnerability management (46% vs. 30% of SMBs) and SecOps case management and ticketing (42% vs. 32%).



Question text: Which of the following threat detection and response activities has your organization automated successfully (e.g., human effort has been reduced while effectiveness has remained consistent or increased)? (Percent of respondents, N=430, multiple responses accepted)

Select Differences in the TD&R Automation, by TD&R Capabilities

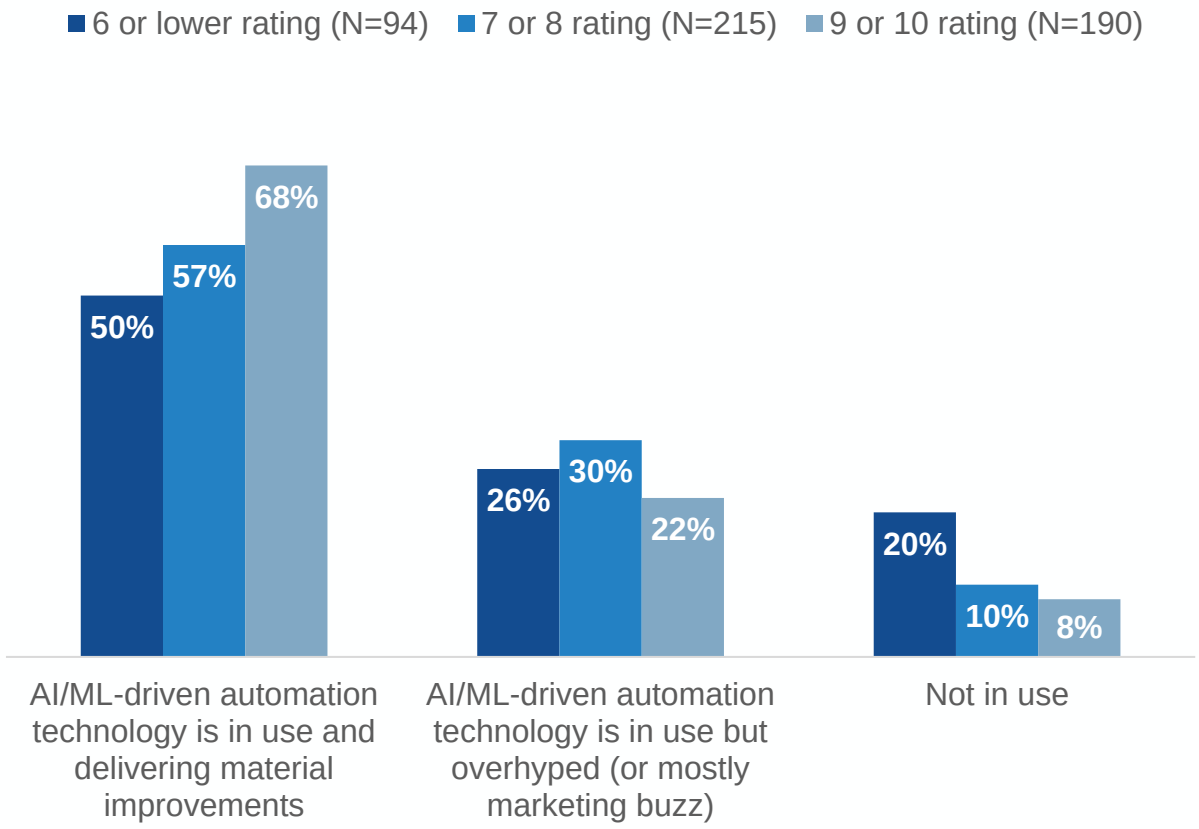
There are several areas where automation success is correlated with TD&R capabilities overall. For example, organizations with the best TD&R practices are more than twice as likely as their peers to have successfully automated SecOps case management.



Question text: Which of the following threat detection and response activities has your organization automated successfully (e.g., human effort has been reduced while effectiveness has remained consistent or increased)? (Percent of respondents, multiple responses accepted)

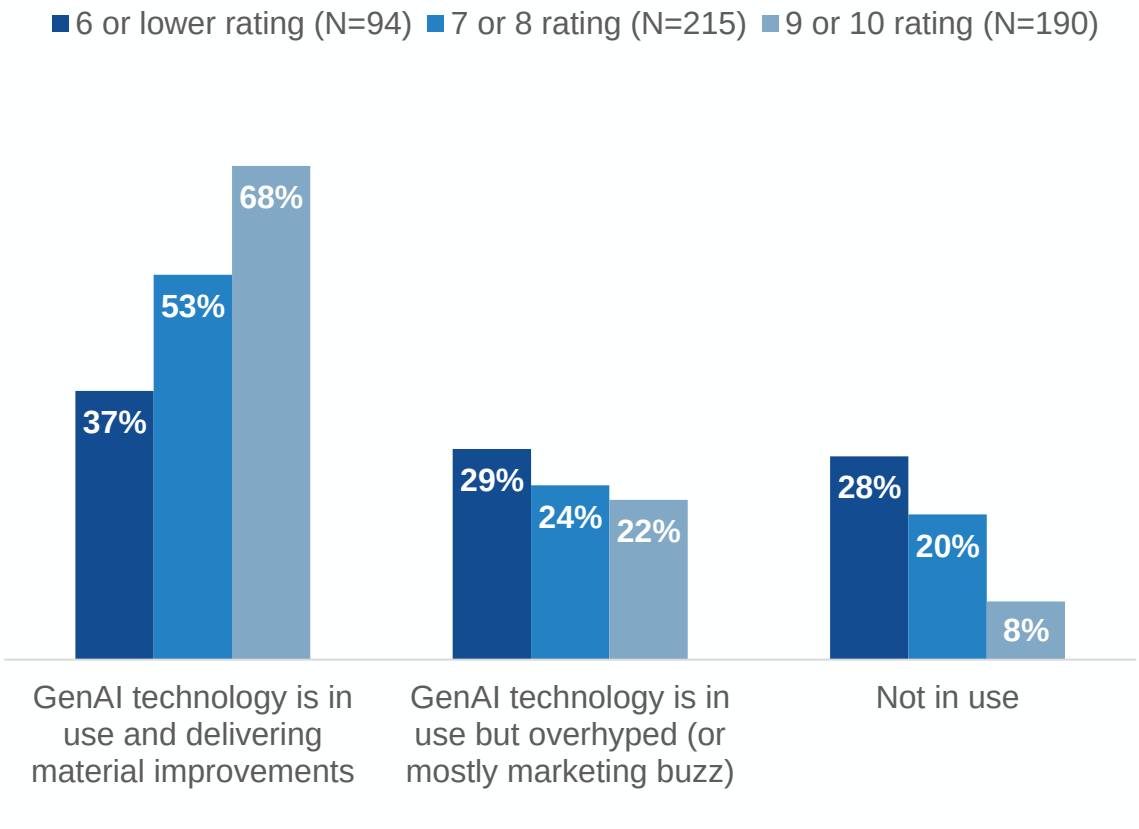
Organizations' Application of AI Technologies to Detect and Respond to Threats

Use of AI/ML-driven automation technologies



Question text: What best describes the use of artificial intelligence/machine learning-driven automation technology for TD&R at your organization? (Percent of respondents)

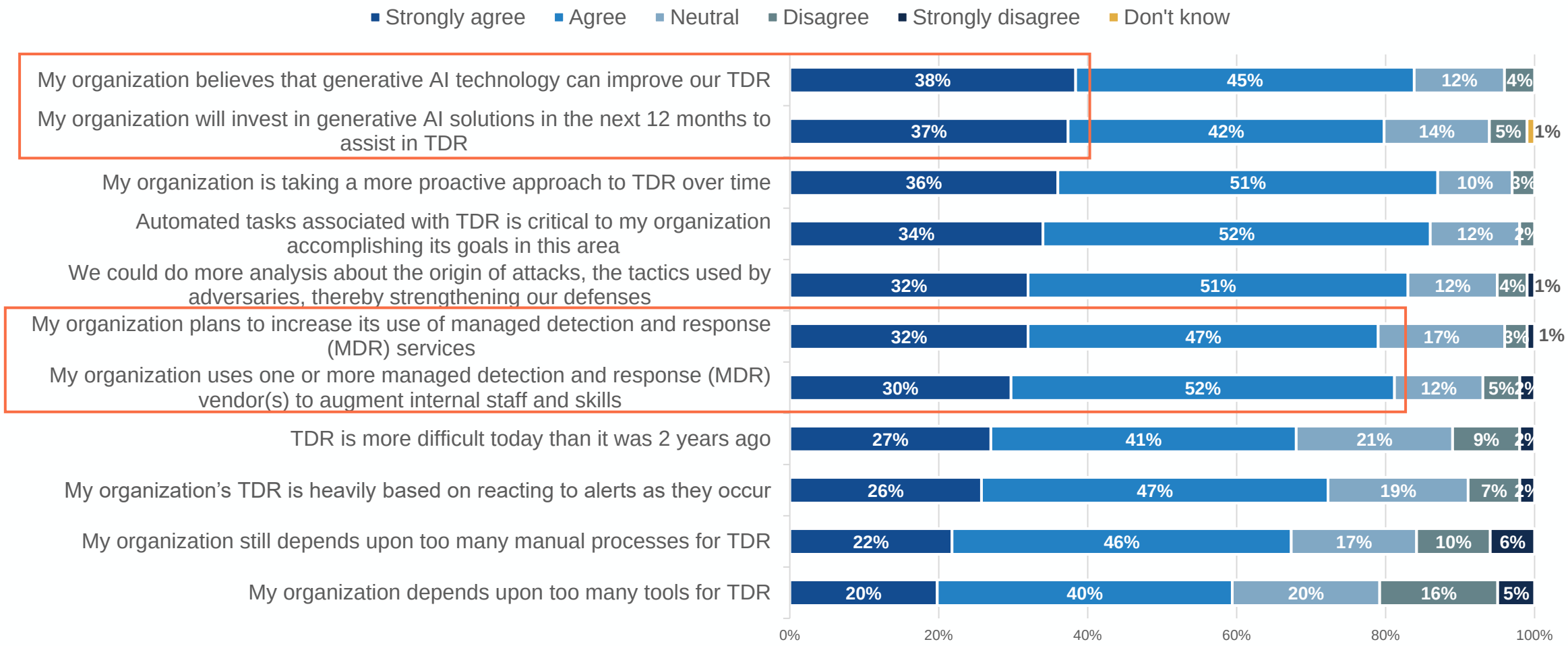
Use of GenAI technologies



Question text: What best describes the use of GenAI technology for TD&R at your organization? (Percent of respondents)

Agreement with a Multitude of Statements Related to the Threat Detection and Response Run High

GenAI has quickly captured a high degree of mindshare; Additionally, 87% of respondents are working toward a more proactive approach, 86% see increased automation as critical, 83% agree they would benefit from more robust root cause analysis processes, and more

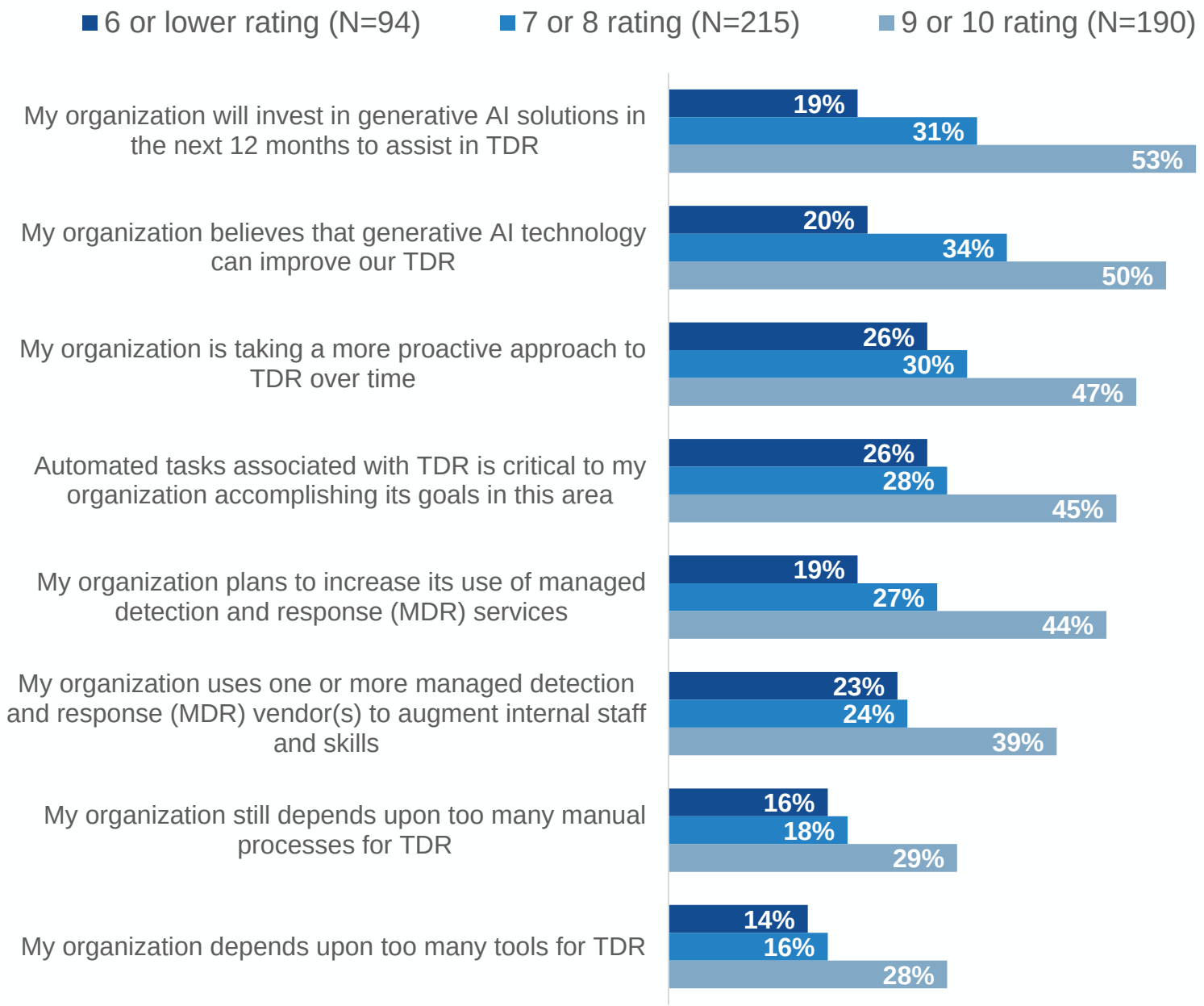


Question text: Please rate your level of agreement with each of the following statements. (Percent of respondents, N=500)

An Organization's TD&R Effectiveness Is Closely Correlated to Several Perceptions and Actions

Organization's most effective at TD&R are:

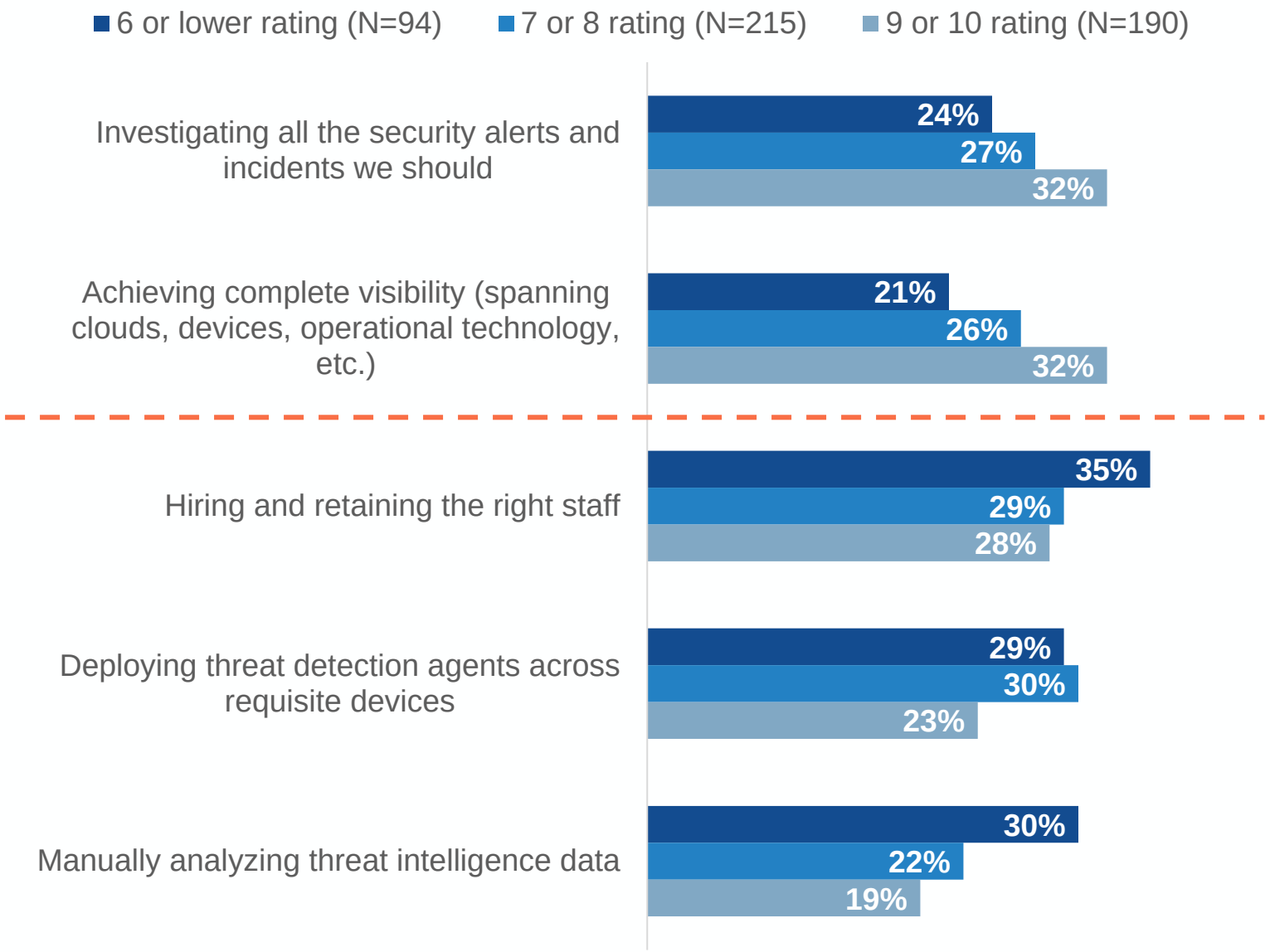
- 2.8x as likely to be planning investments in GenAI for TD&R
- 2.3x as likely to be planning to ramp up use of MDR
- 2x as likely to feel TD&R tool rationalization is needed
- And more



Question text: Please rate your level of agreement with each of the following statements.: (Percent of respondents, "strongly agree" respondents only

Select Differences in Challenges, by TD&R Capabilities

Organizations strong on TD&R more often struggle with alert fatigue and complete visibility across their IT estate; Organizations weak on TD&R more often struggle with staffing, device coverage, and manual TI analysis.



Question text: Which of the following threat detection and response activities are most challenging for your organization? (Percent of respondents, up to three responses accepted)

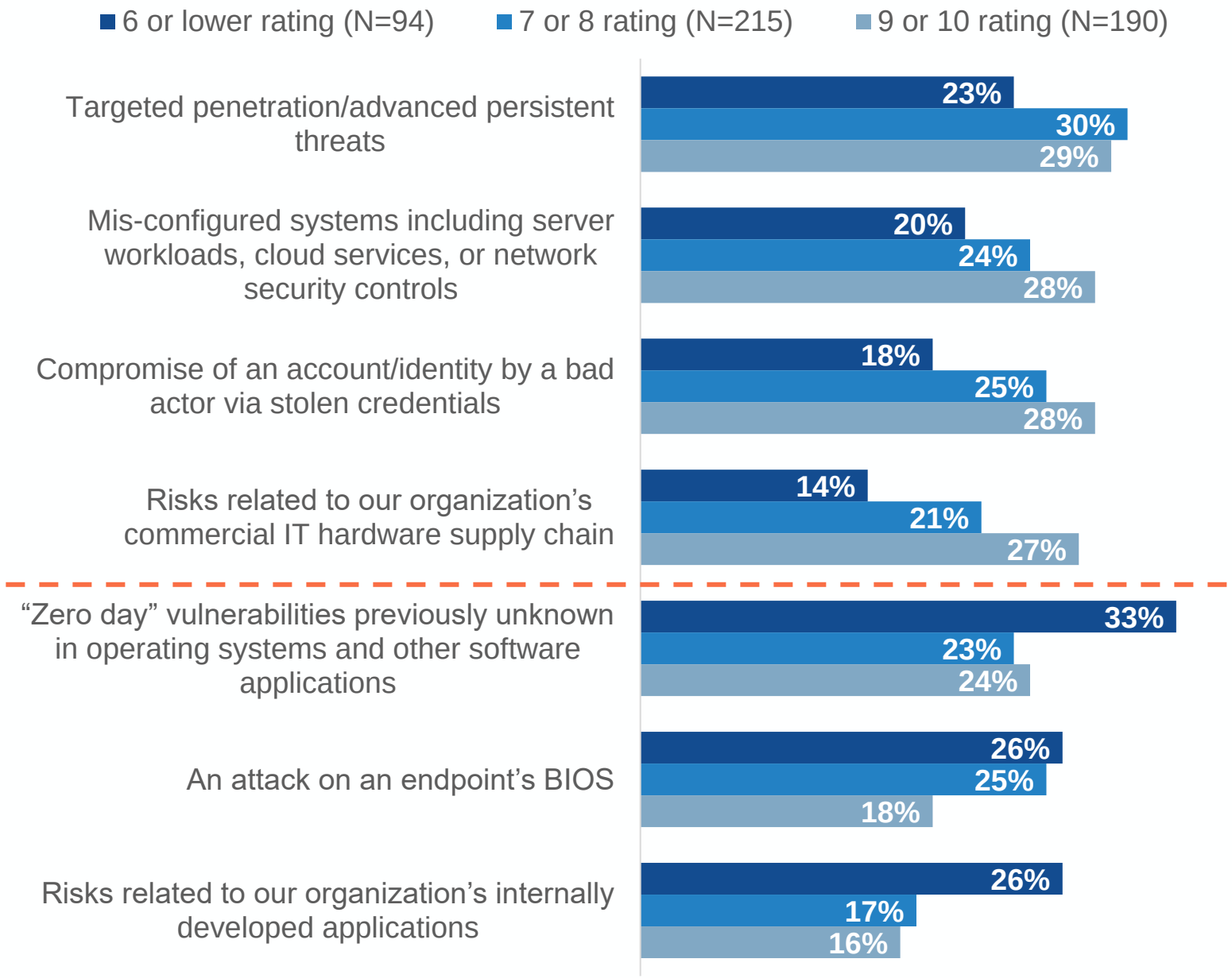
Vulnerabilities abound with targeted attacks being seen as the most concerning vulnerability

C-level respondents are worried are particularly worried about targeted attacks (39% vs. 26% of management).

Question text: Which of the following threat vectors would you say your organization is most vulnerable to a significant cyber-attack? (Percent of respondents, N=500, three responses accepted)

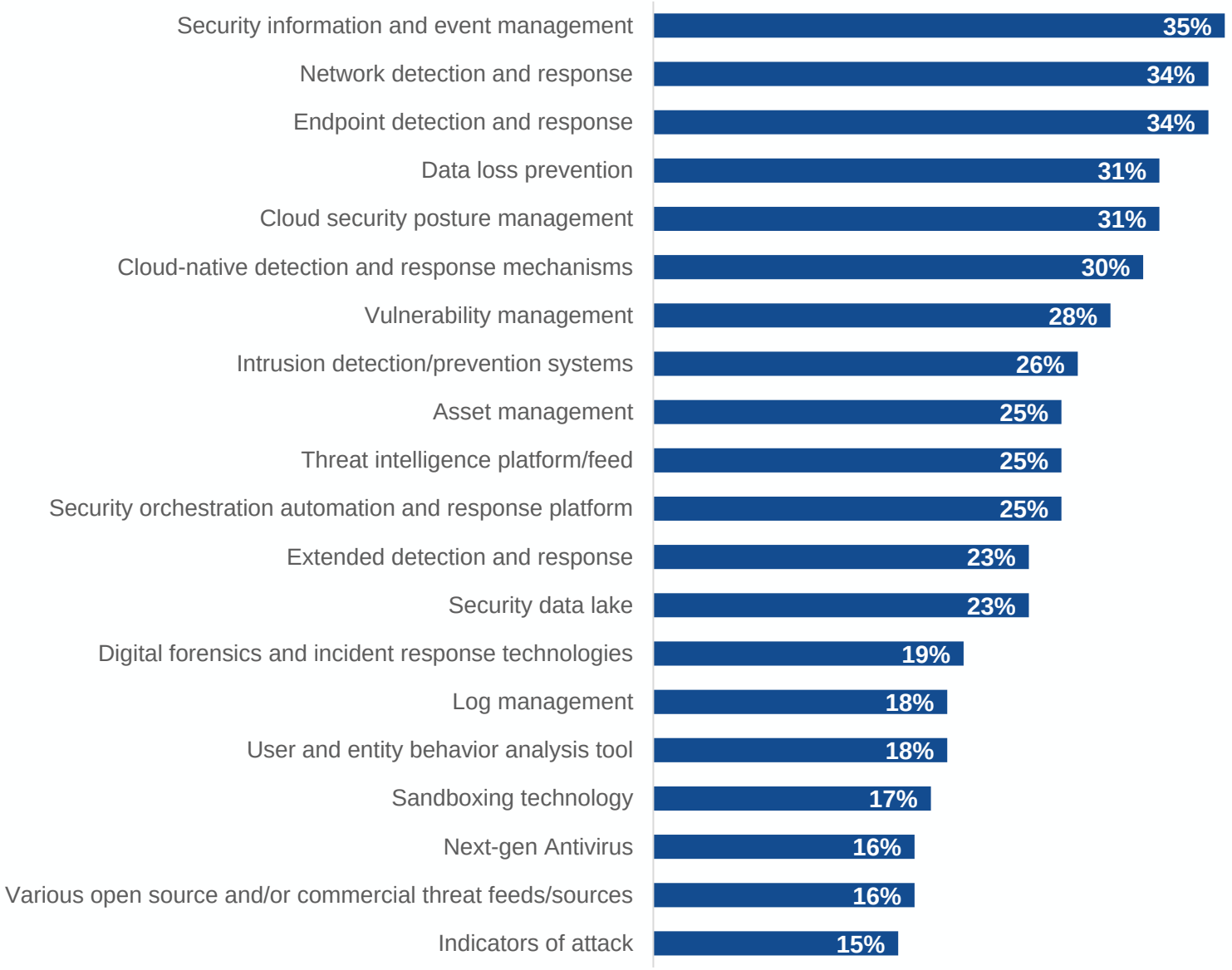
Differences in Perceived Vulnerability, by TD&R Capabilities

Differences in perception may be an indicator of where organizations are on their journeys. For example, less organizations with less sophisticated TD&R capabilities are more apt to fear zero day vulns while more advanced organizations prioritize credential theft and their IT hardware supply chain.



Question text: Which of the following threat vectors would you say your organization is most vulnerable to a significant cyber-attack? (Percent of respondents, up to three responses accepted)

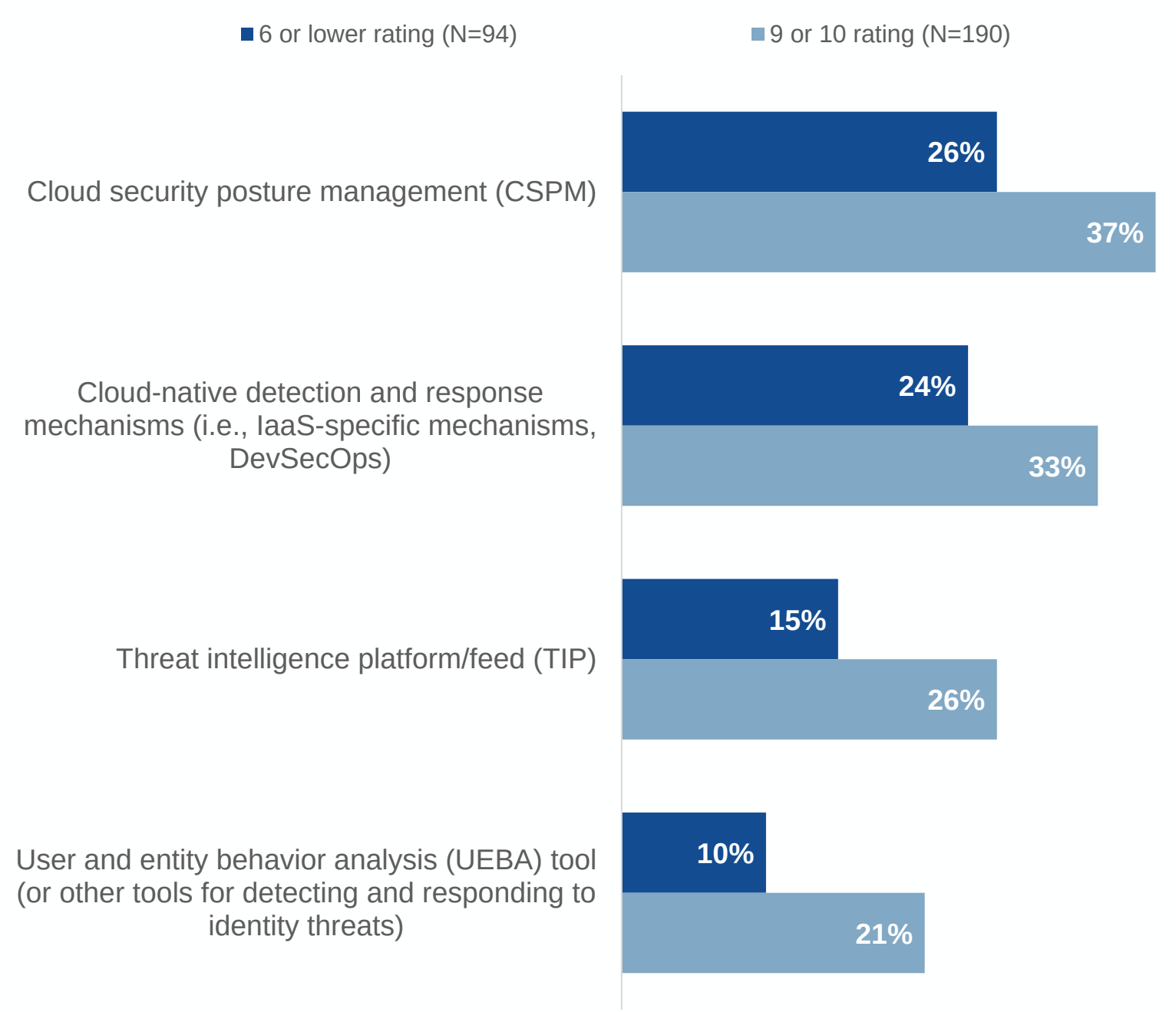
Data Sources Used to Support TD&R Activities



Question text: Which of the following technologies does your organization currently use data/telemetry from to detect and respond to threats? (Percent of respondents, N=500, multiple responses accepted)

Stronger TD&R Capabilities Appear to be Enabled by Using more Data Sources

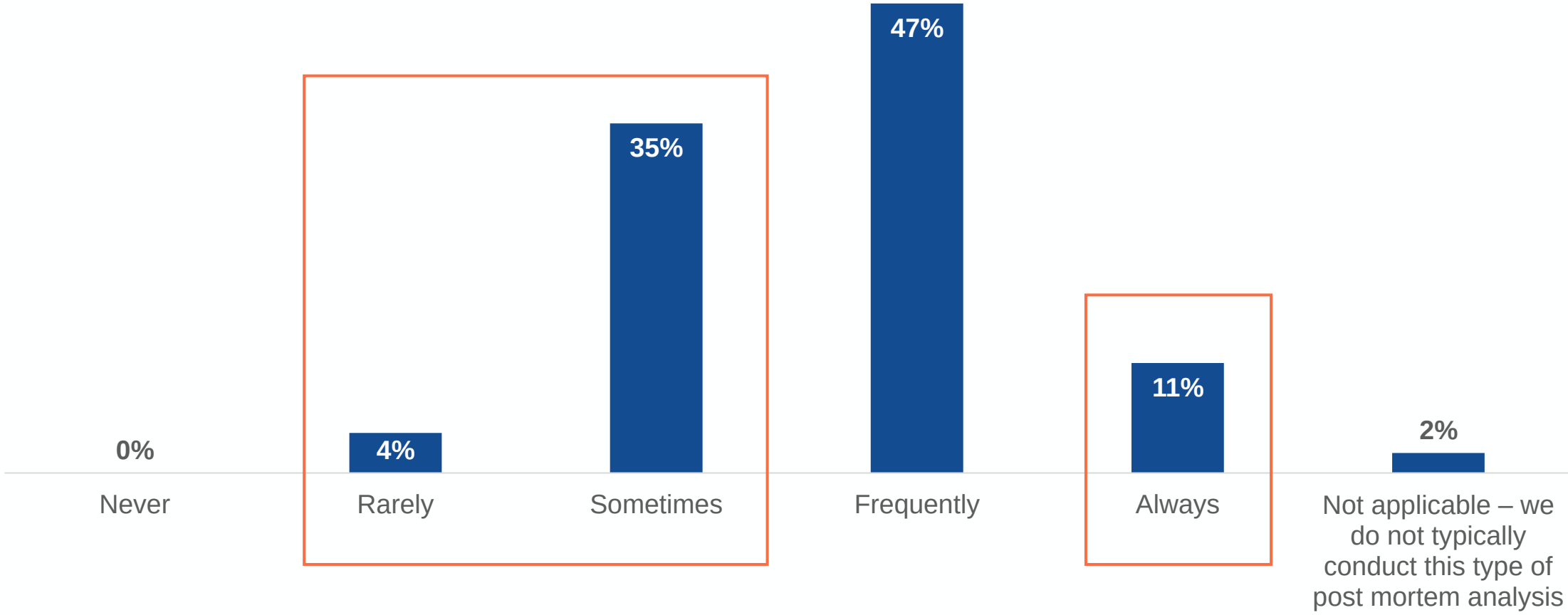
Leaders in this area report using several sources much more often.



Question text: Which of the following technologies does your organization currently use data/telemetry from to detect and respond to threats? (Percent of respondents, multiple responses accepted)

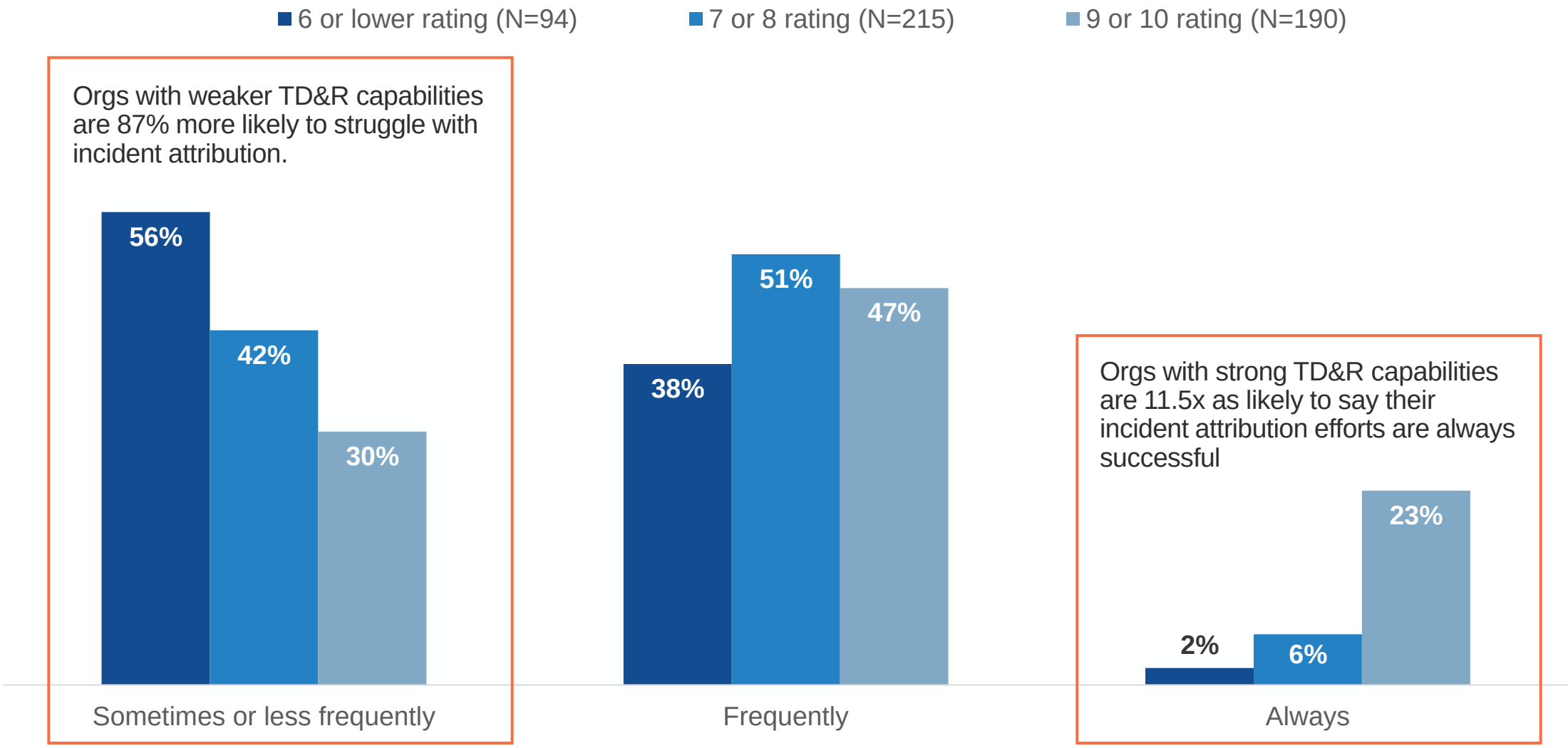
Success Discovering Root Causes in Postmortem Analyses

89% of organizations say at least some of their postmortem analyses of incidents fail to uncover incidents' root cause; two in five respondents report significant gaps in their ability to attribute incident causes.



Question text: In the process of investigating incidents, how frequently would you estimate your organization is able to attribute the origination of the incident to a specific endpoint and end-user action? (Percent of respondents, N=500)

Incident Attribution Success, by TD&R Capabilities

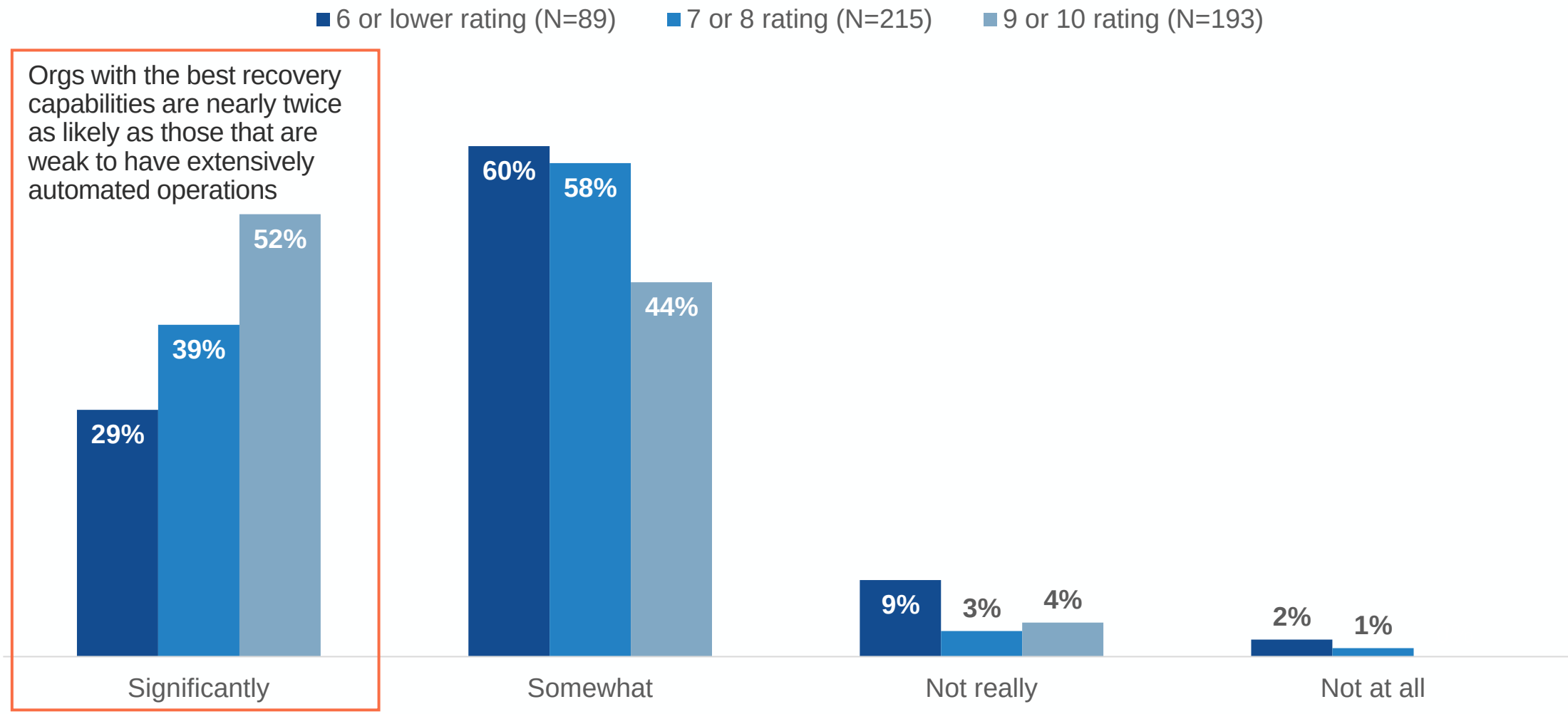


Question text: In the process of investigating incidents, how frequently would you estimate your organization is able to attribute the origination of the incident to a specific endpoint and end-user action? (Percent of respondents)

Attack Recovery Insights

Enterprise Strategy Group™
by TechTarget

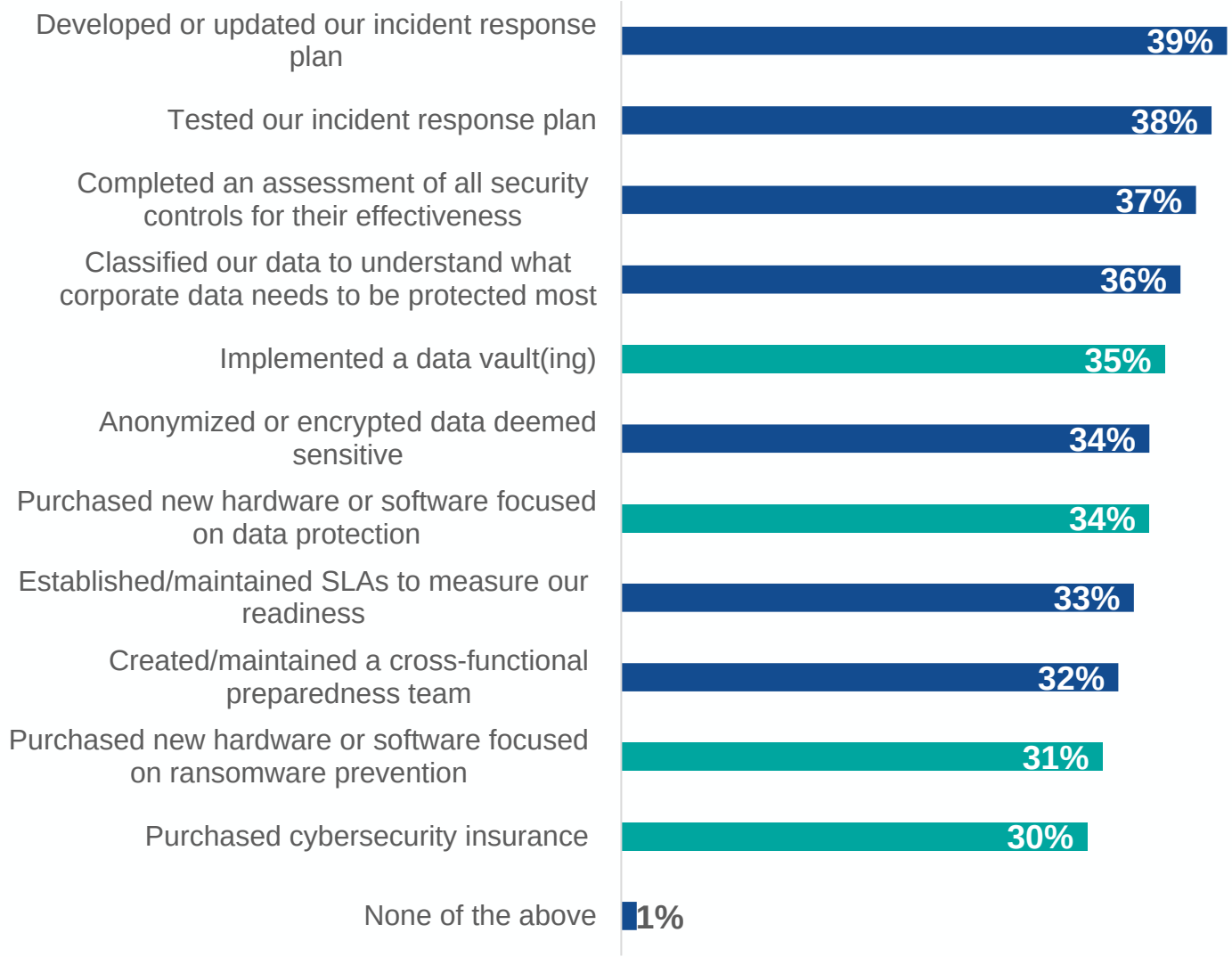
Evaluating Attack Recovery, Automation Continues to be an Indicator of Program Pillar Strength



Question text: To what degree are/would professional/managed services be utilized for incident response planning and cyber-attack recovery within your organization? (Percent of respondents)

Actions Taken to for Disruptive Attacks

No one set of actions dominate, but **procedural** preparation seems to outstrip new **technology/solution** purchases.

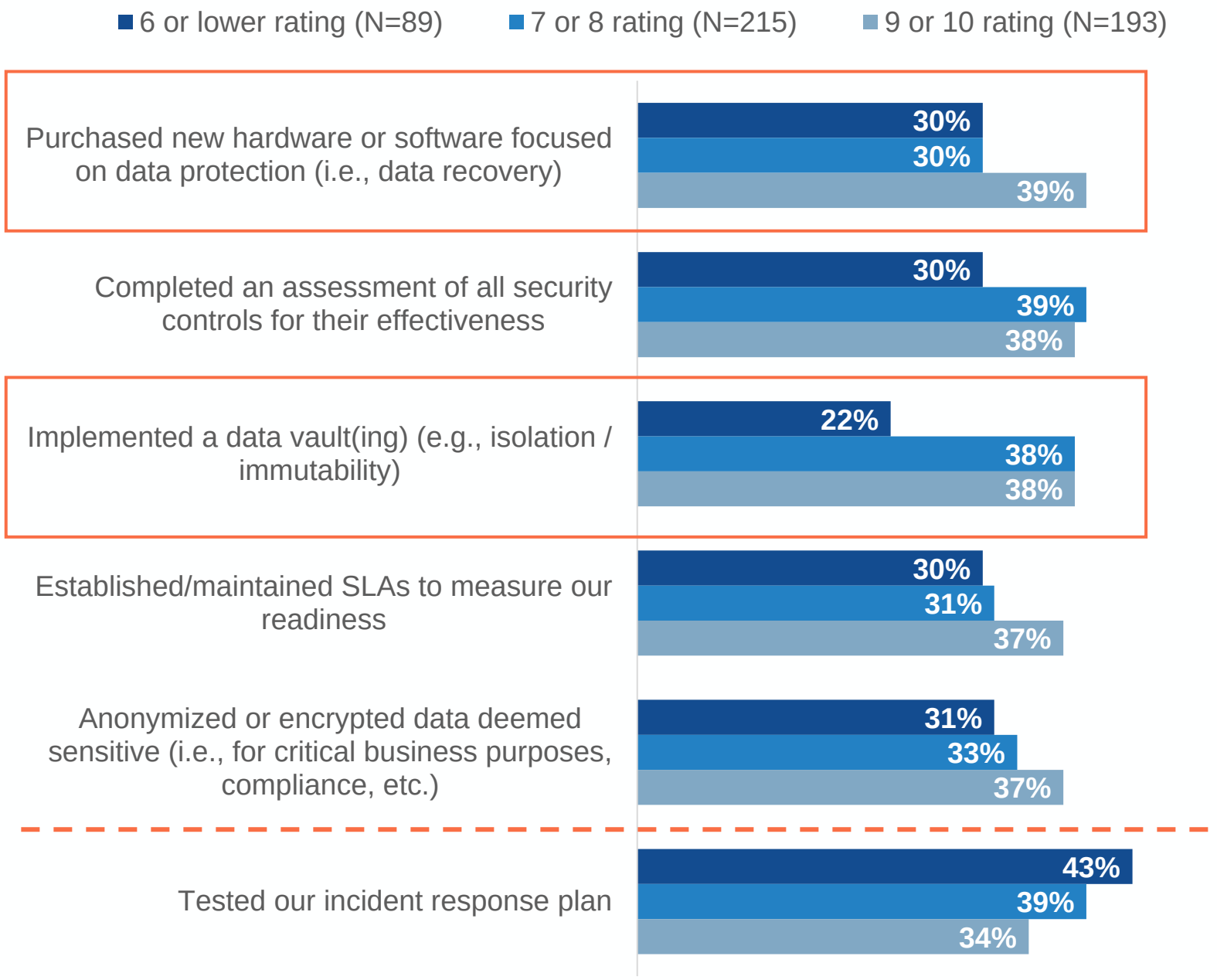


Question text: What specific formal readiness measures has your organization taken in the last 12 months to prepare for a disruptive cyber-attack (e.g., a ransomware attack targeting business-critical data/apps)? (Percent of respondents, N=500, multiple responses accepted)

How Attack Recovery Preparation Activities Vary by Attack Recovery Capabilities

Organizations stronger on attack recovery have taken more steps to prepare, including purchasing new data recovery and vaulting technologies.

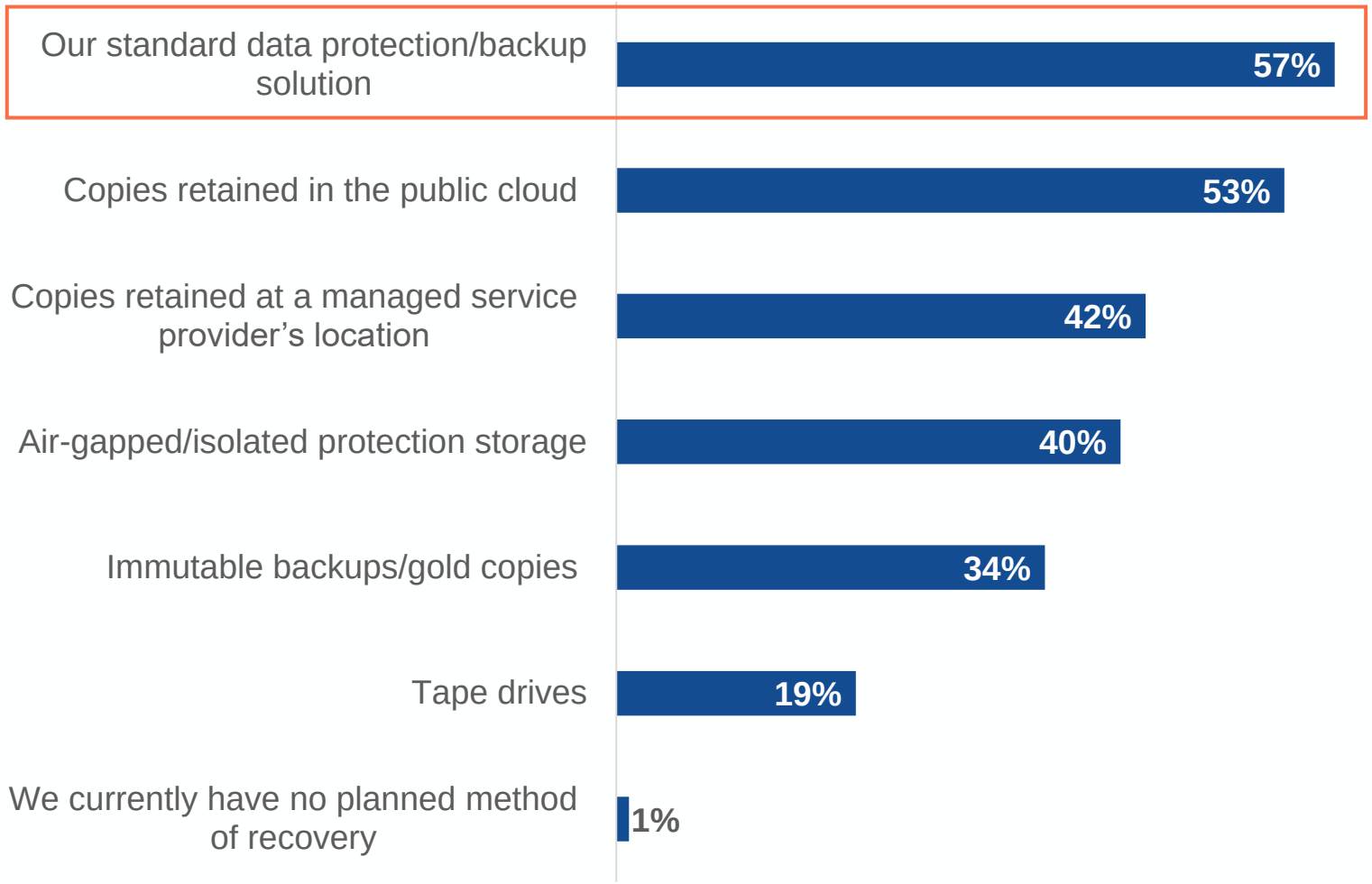
Leaders are 30% more likely to have invested in new data recovery technology and 72% more likely to have invested in data isolation/immutability technologies in the past 12 months.



Question text: What specific formal readiness measures has your organization taken in the last 12 months to prepare for a disruptive cyber-attack (e.g., a ransomware attack targeting business-critical data/apps)? (Percent of respondents, multiple responses accepted)

Where Organizations Retain their Data for Recovery

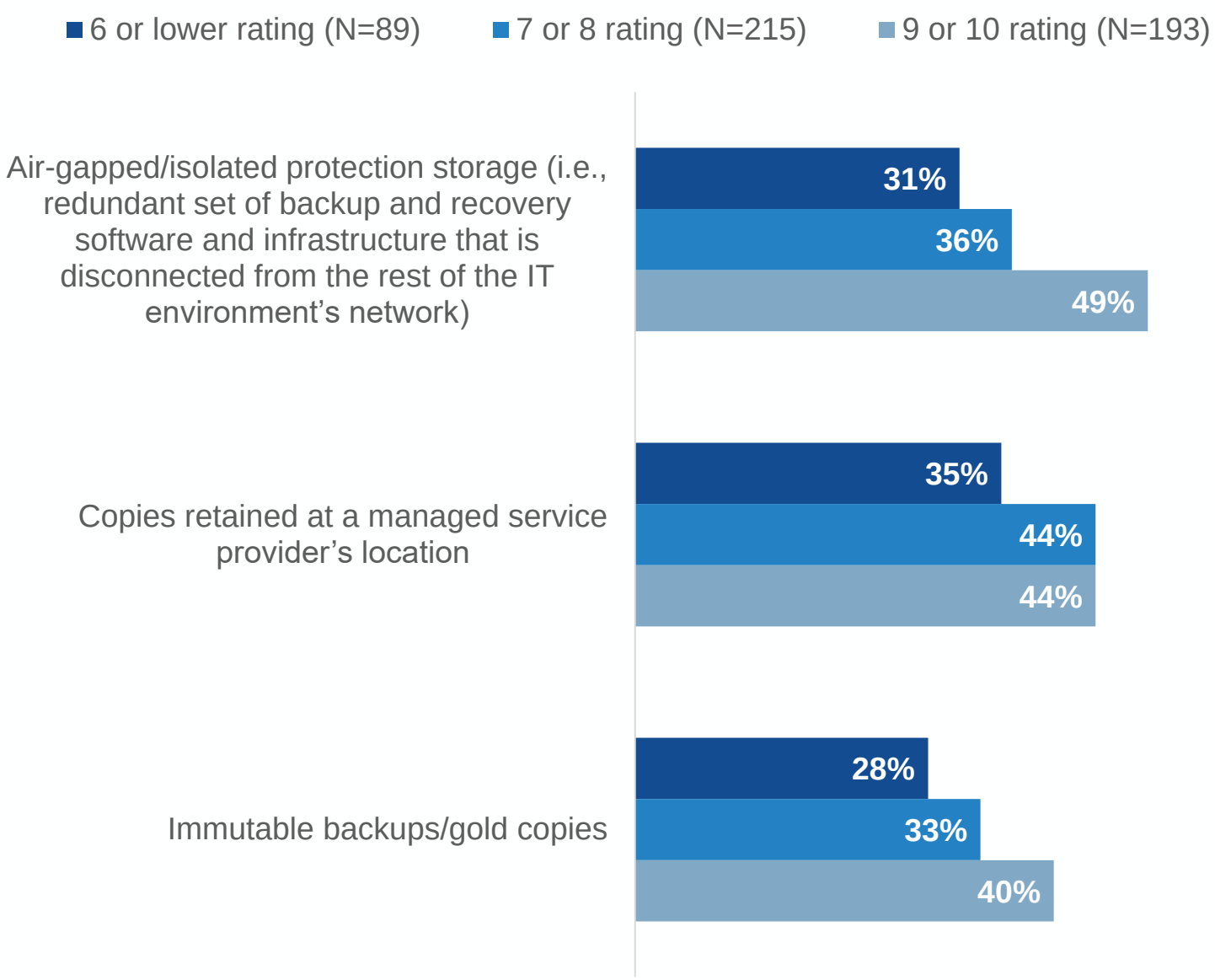
Standard backup solutions are still the predominant cyber recovery medium.



Question text: Where are your organization's mission-critical data assets stored for cyber recovery? (Percent of respondents, N=500, multiple responses accepted)

Organizations with Stronger Recovery Capabilities Have More Often Deployed Specialized Solutions, Engaged Third Parties

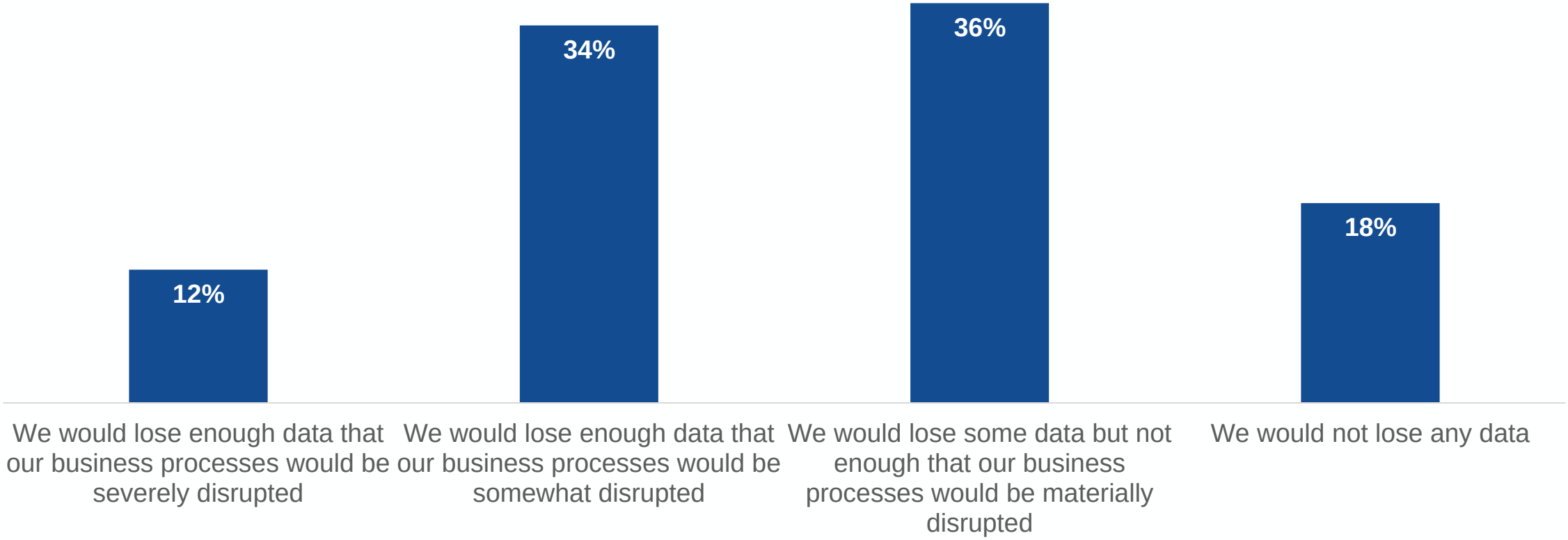
They are 58% more likely to have deployed air-gapped storage, 42% more likely to leverage immutable backup technologies, and 26% more likely to store copies of data with MSPs.



Question text: Where are your organization's mission-critical data assets stored for cyber recovery? (Percent of respondents, multiple responses accepted)

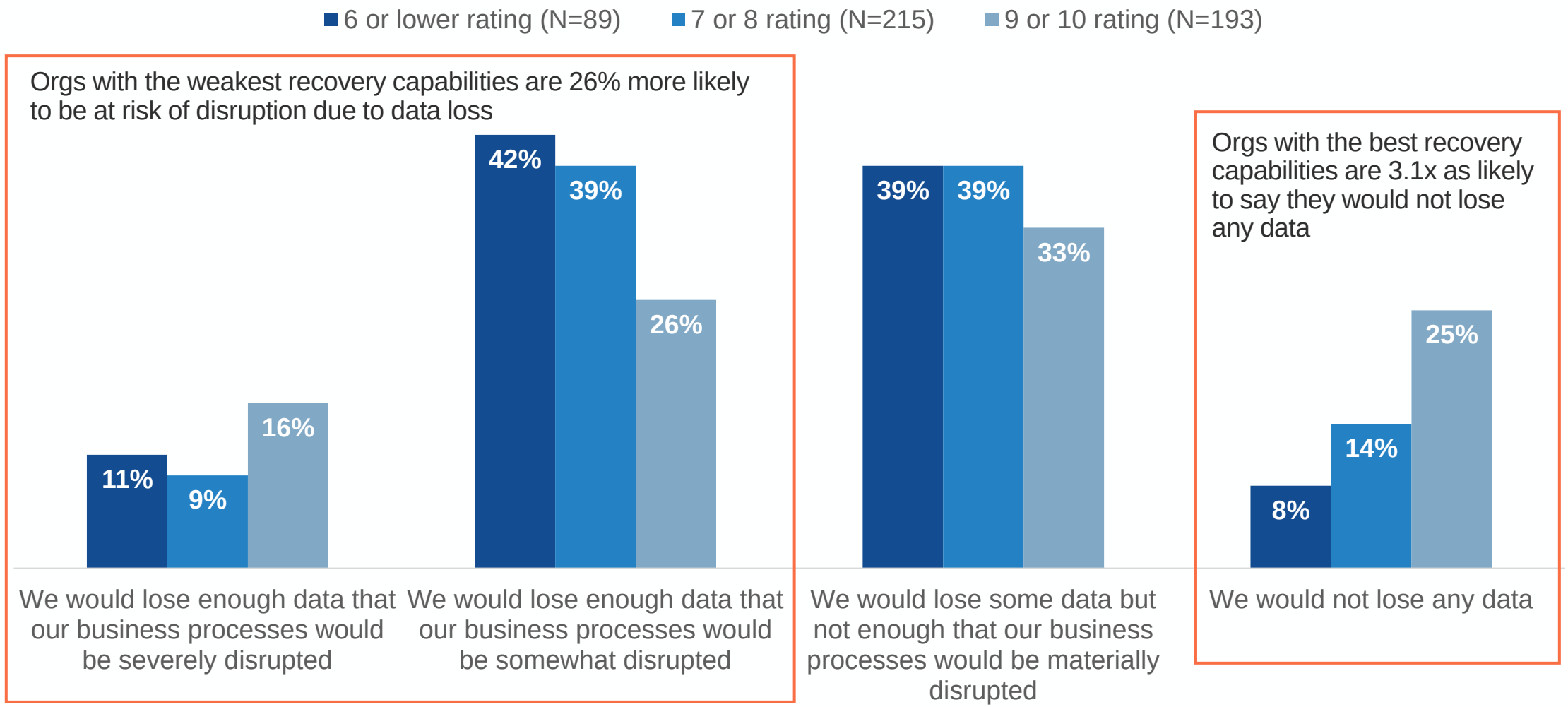
Expectations for Data Loss

Less than 1 in 5 respondents expect they would recover all their data after a major attack, 46% respondents expect their business would face material disruption.



Question text: If your organization had to conduct a major recovery as a result of a cyber attack, which best characterizes your expectations around data loss? (Percent of respondents, N=500)

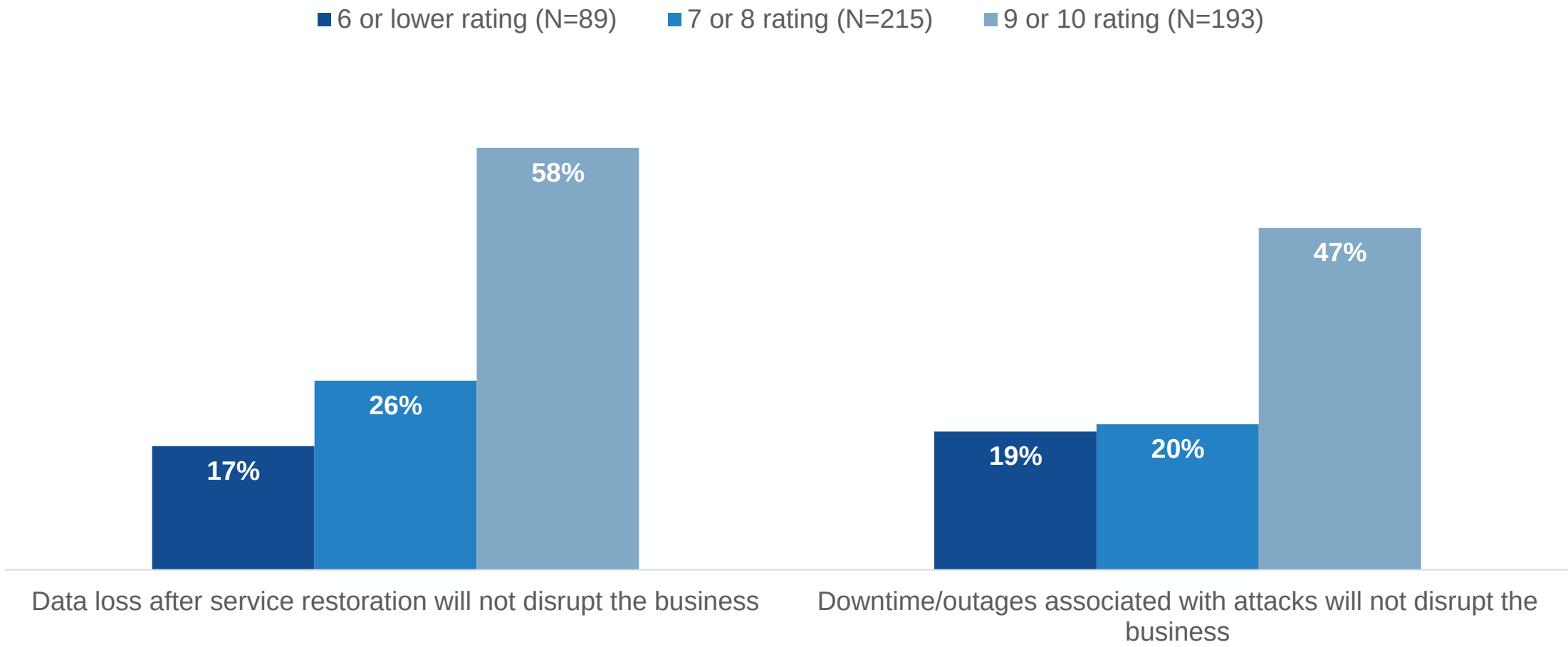
Expectations for Data Loss, by Cyber Attack Capabilities



Question text: If your organization had to conduct a major recovery as a result of a cyber attack, which best characterizes your expectations around data loss? (Percent of respondents)

Confidence Related to Avoiding Business Disruption in the Event of an Attack, by Attack Recovery Capabilities

Leaders in this pillar are 3.4x as likely to be very confident they can recover completely enough after an attack that they would avoid disruption; they are also 2.5x as likely to say they can recover from attacks fast enough to avoid disruption.



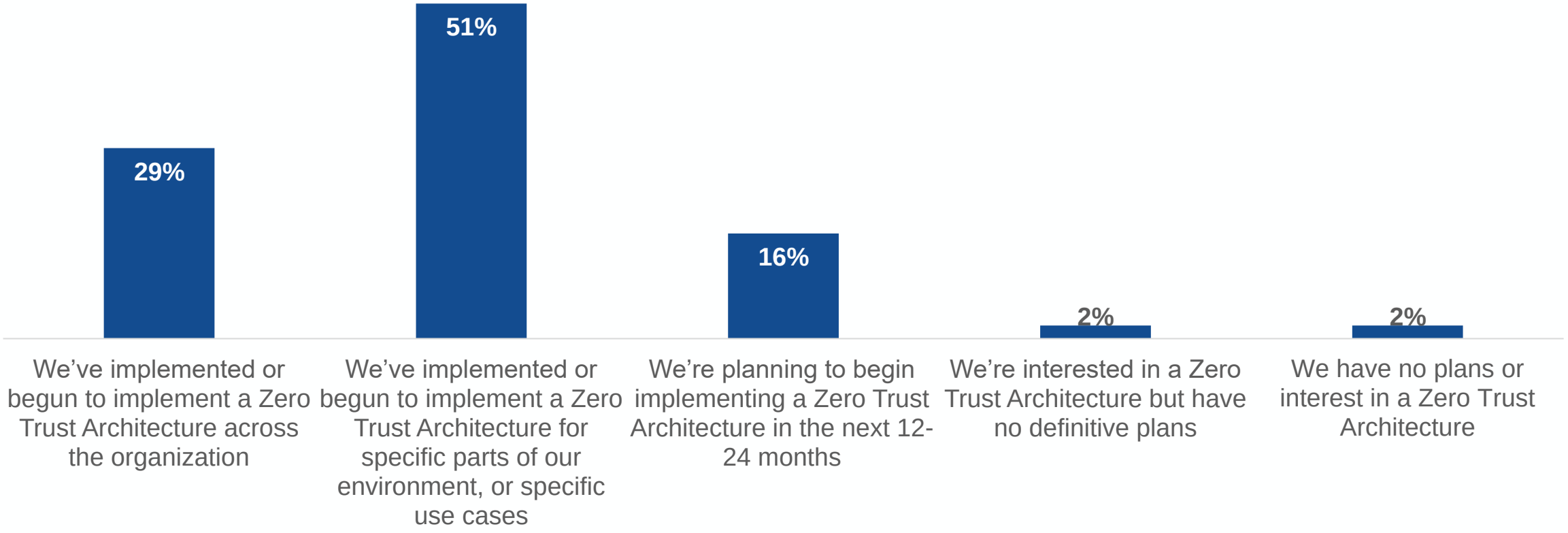
Question text: Based on your organization's readiness how confident are you that…: (Percent of respondents, "very confident" respondents only)

The State of Zero Trust

Enterprise Strategy Group™
by TechTarget

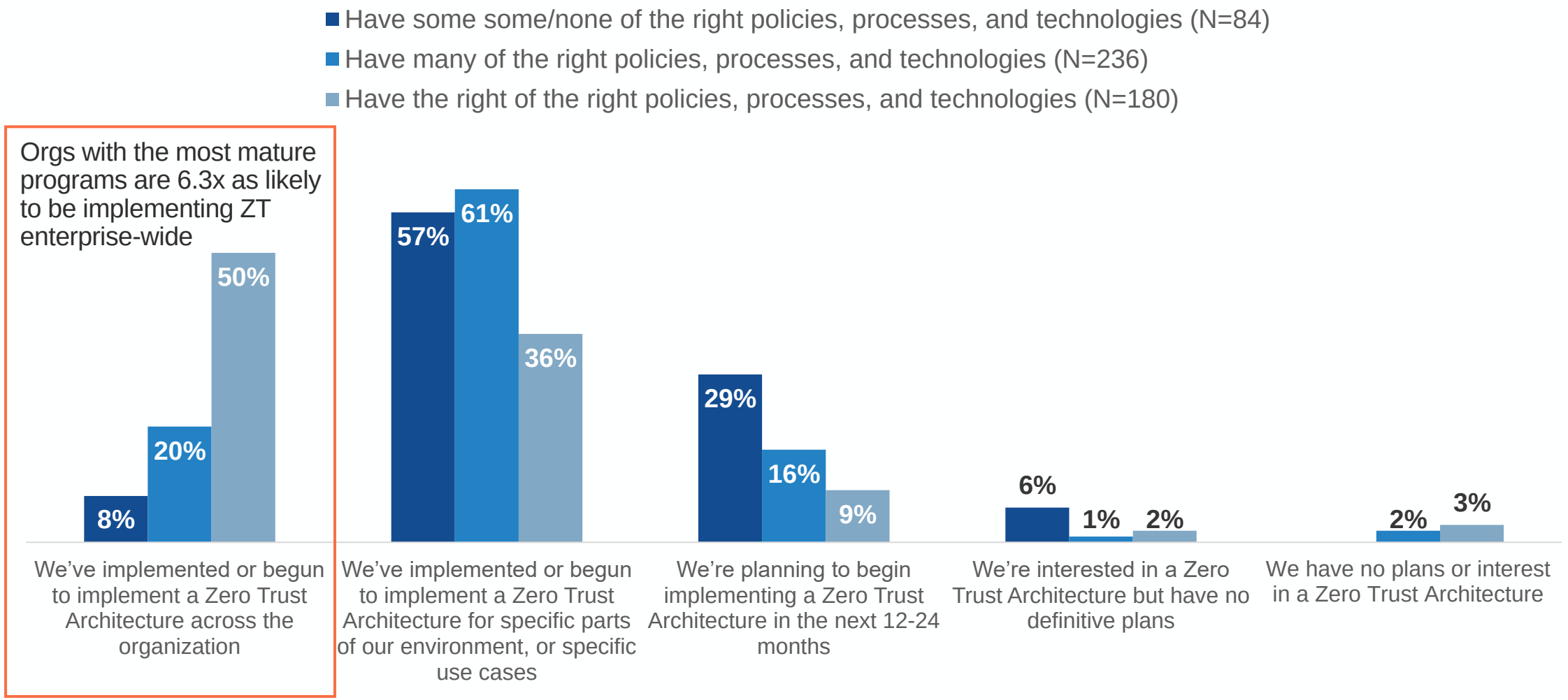
How Far Down the Zero Trust Path Are Organizations Today?

Just 2% of organizations are eschewing a Zero Trust architecture, most organizations (51%) are in the early stages of adoption, while 29% report and enterprise-wide implementation is in progress.



Question text: Which of the following statements best reflects your organization's adoption of a Zero Trust Architecture? (Percent of respondents, N=500)

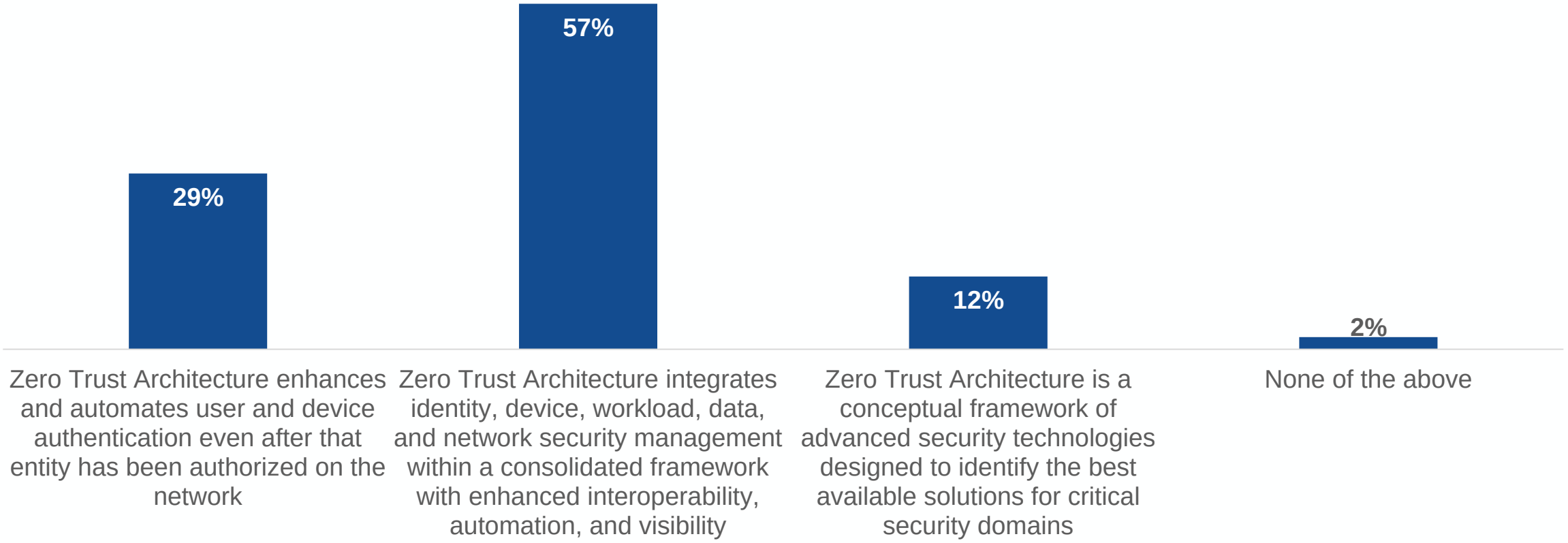
Organizations with Mature Cybersecurity Programs Are More Aggressively Adopting Zero Trust Architectures



Question text: Which of the following statements best reflects your organization's adoption of a Zero Trust Architecture? (Percent of respondents)

What Does Zero Trust Mean to Respondents?

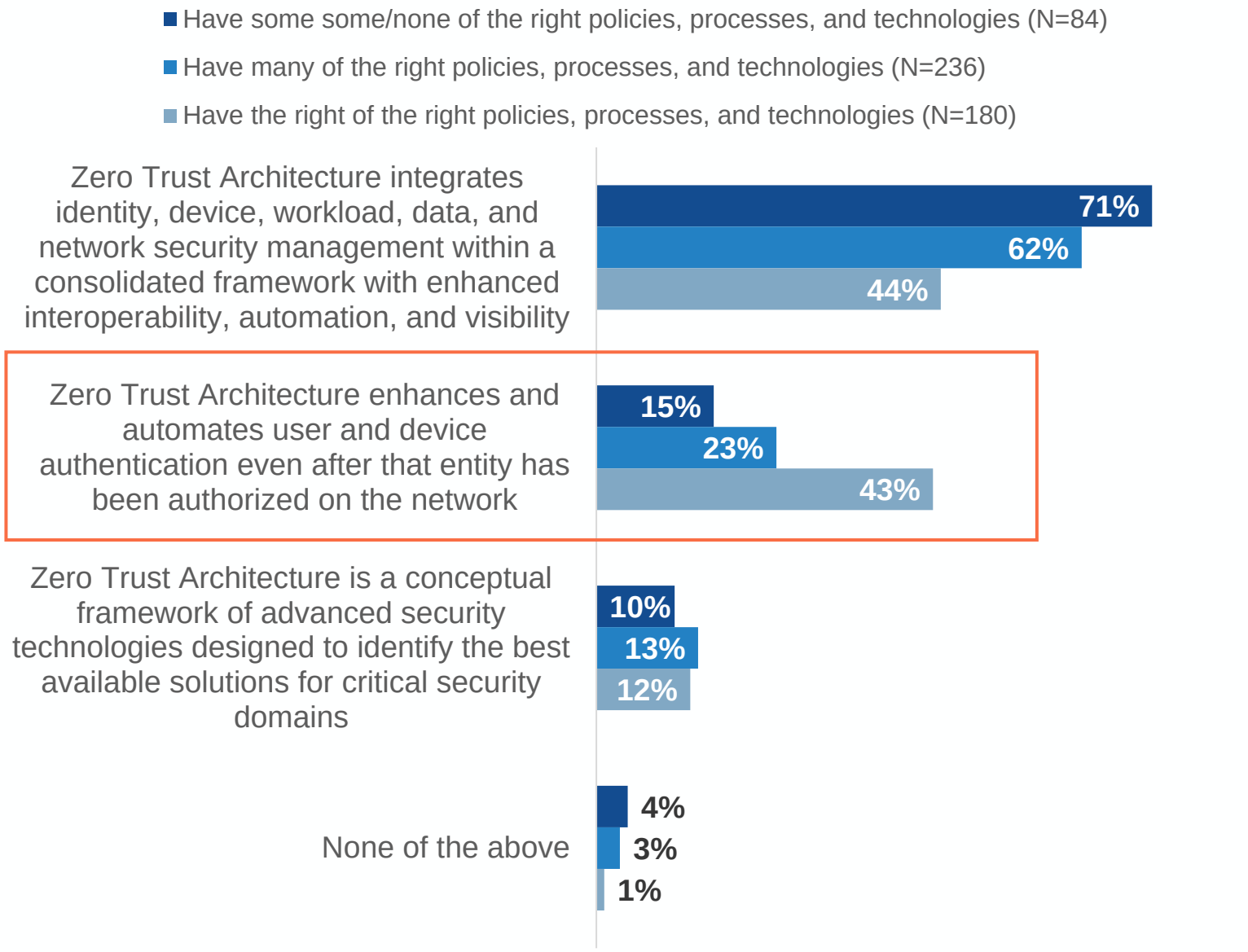
The majority of respondents associate Zero Trust with a consolidated framework for security management that spans the entire environment.



Question text: Which of the following statements is most closely aligned with your organization's definition of a Zero Trust Architecture? (Percent of respondents, N=500)

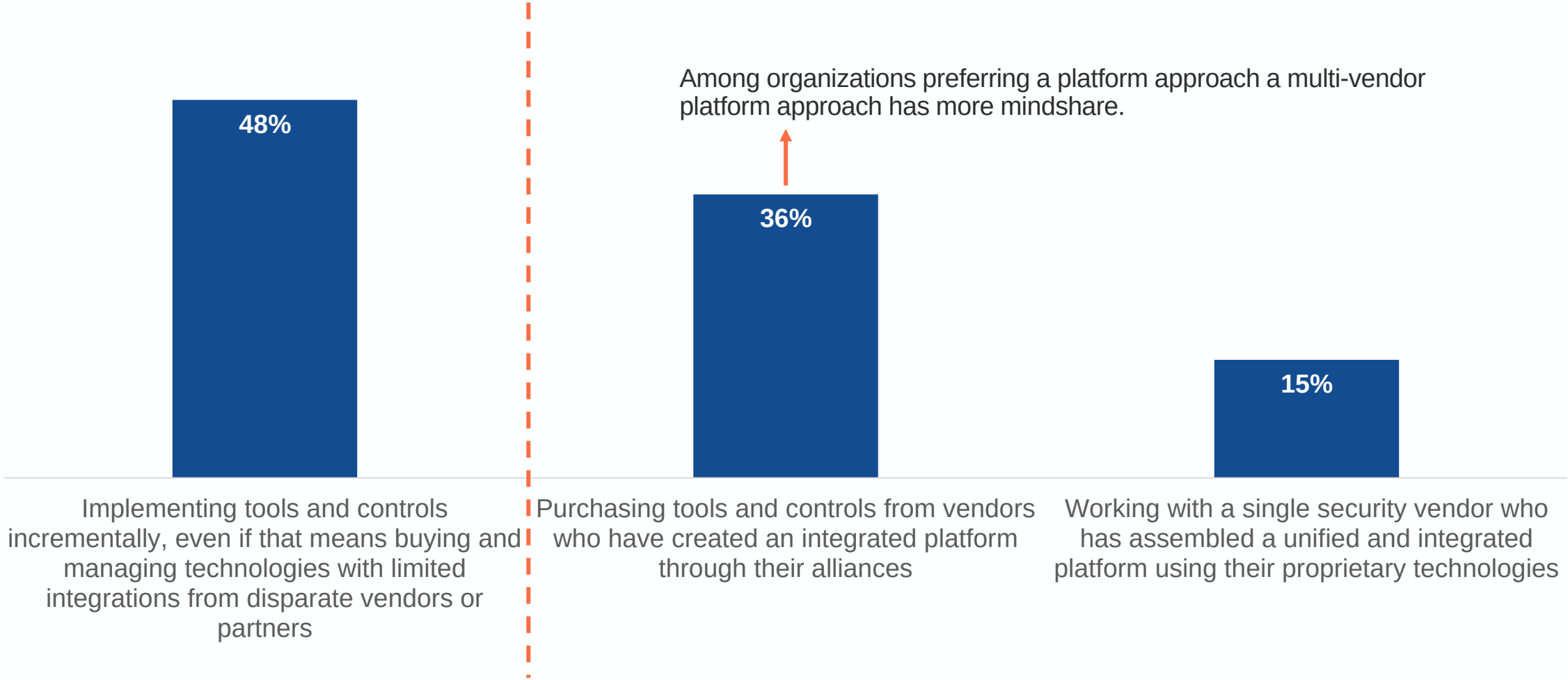
How Zero Trust Perception Varies by Cybersecurity Program Maturity

For organizations with the most mature cybersecurity programs, the concept continuous, automated authentication after authorization resonates.



Question text: Which of the following statements is most closely aligned with your organization's definition of a Zero Trust Architecture? (Percent of respondents)

Approaches to Furthering Zero Trust Initiatives Are Varied with Nearly Half the Market Preferring a Point-Tool Approach

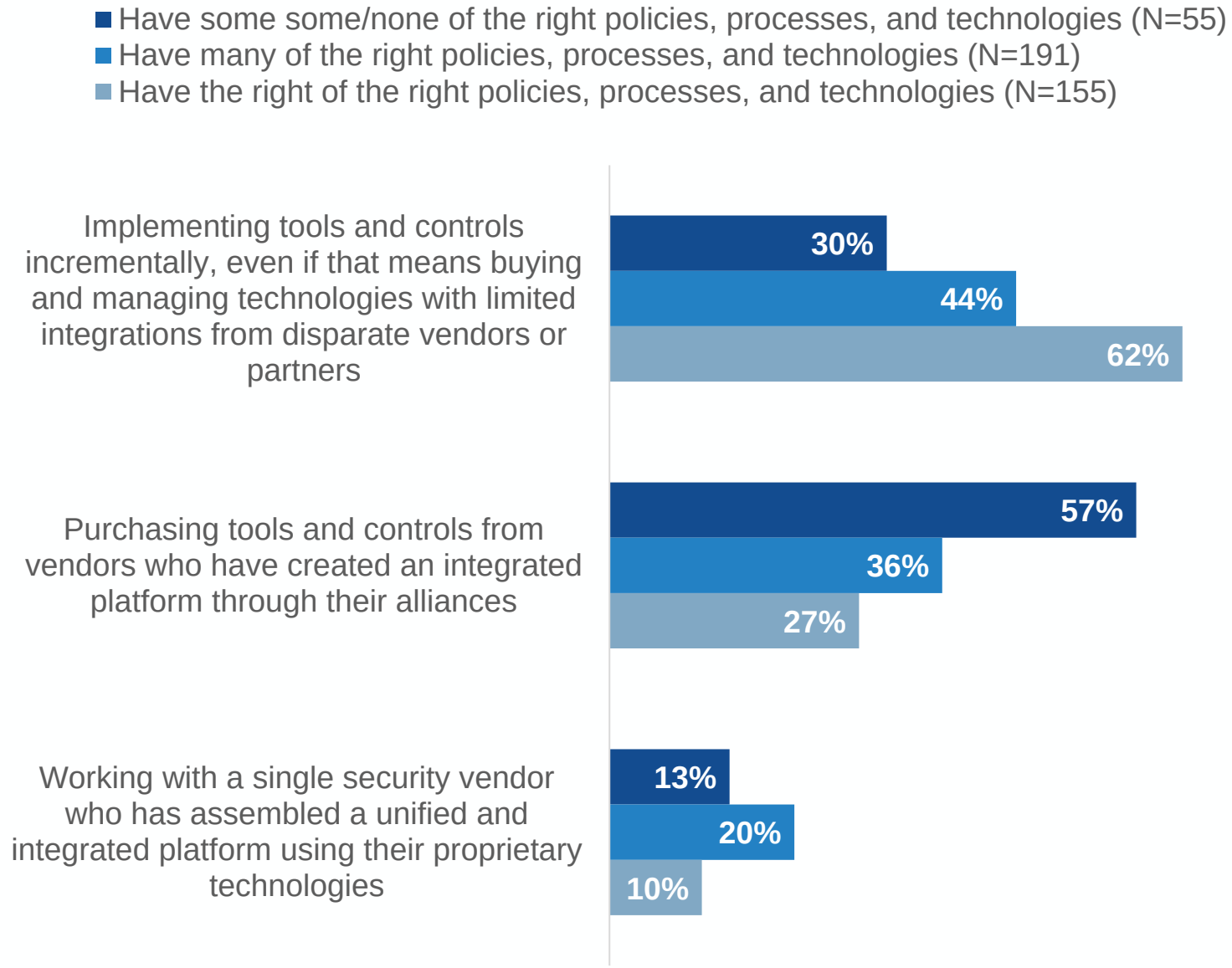


Question text: When it comes to furthering Zero Trust initiatives, what does your organization prefer? (Percent of respondents, N=479)

Zero Trust Adoption Preferences Vary by Cybersecurity Program Maturity

More mature organizations feel more capable of stitching together a best-of-breed approach to Zero Trust.

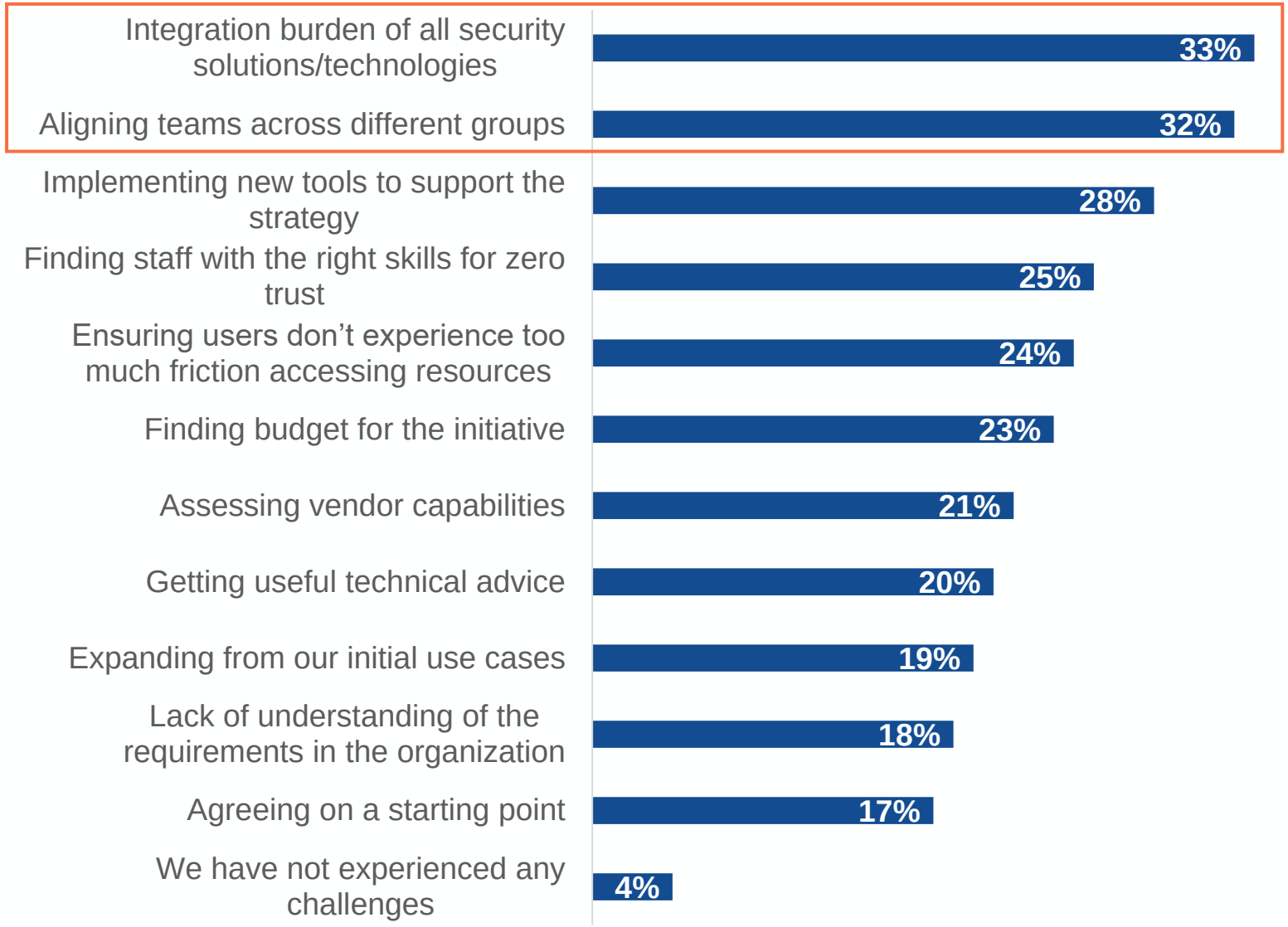
Less mature organizations are more apt to see the appeal of pre-integrated solutions.



Question text: When it comes to furthering Zero Trust initiatives, what does your organization prefer? (Percent of respondents)

Challenges Organizations Are Encountering on their Zero Trust Journeys

Thematically, cohesion (spanning both teams and technology) is a top challenge organizations encounter as they employ Zero Trust architecture approaches.



Question text: What have been your organization's greatest challenges with regards to its zero trust initiative(s)? (Percent of respondents, N=401, three responses accepted)

Challenges Associated with Zero Trust, by Cybersecurity Program Maturity

While in general challenges are similar regardless of program maturity, organizations with stronger cybersecurity programs tend to need more help achieving cross-team alignment (34% vs. 24%) and organizations with weaker cybersecurity programs tend to grapple more with budget shortfalls (31% vs. 15%).

Question text: What have been your organization's greatest challenges with regards to its zero trust initiative(s)? (Percent of respondents, up to three responses accepted)

Thank you

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.